

1. OBJET DES CGU

Les présentes CGU ont pour objet de préciser le contenu et les modalités d'utilisation des Certificats de signature cachet délivrés par l'AC « BE-YS CUSTOMER SERVICES CA NB » ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les Certificats Customer Services sont utilisés dans le cadre du déploiement du Service de signature cachet proposé par be-invest à ses Clients et à leurs Utilisateurs ou bien dans le cadre du service d'horodatage be-ys.

Les Certificats de signature Cachet émis par l'AC « BE-YS CUSTOMER SERVICES CA NB » sont des Certificats à destination des Clients, personnes morales ou unités d'horodatage, du Service de signature cachet mis en œuvre par be-invest.

La Bi-clé de signature cachet est stockée de manière sécurisée dans un Module cryptographique matériel hébergé dans les locaux sécurisés de l'AC « BE-YS CUSTOMER SERVICES CA NB ».

L'activation sécurisée de la Bi-clé associée à un Certificat de signature cachet permet :

- la signature électronique des informations et documents du Client qui seront présentés aux Utilisateurs via le Service de signature électronique, assurant ainsi l'origine, l'intégrité et la non-répudiation des informations présentées ;
- la signature cachet des demandes d'horodatage pour génération des Contremarques de temps.

2. DEFINITIONS

Applications utilisatrices : Services applicatifs exploitant les Certificats émis par l'AC « BE-YS CUSTOMER SERVICES CA NB », par exemple, pour des besoins de vérification de signature cachet.

Autorité de Certification (AC) : Entité qui délivre et est responsable des Certificats électroniques émis et signés en son nom conformément aux règles définies dans sa PC et dans la DPC associée.

Autorité de Gouvernance (AG) : Entité responsable de l'ensemble des fonctions de l'IGC be-ys avec pouvoir décisionnaire.

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 certificats.

Bi-clé : Couple clé publique/ clé privée

Cérémonie des Clés ou Key Ceremony (KC) : Réunion spéciale des personnes autorisées pour générer le certificat de signature cachet. La Bi-clé de ce certificat doit être générée avec toutes les précautions nécessaires pour éviter sa compromission.

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

Client: Entité cliente ayant décidé de souscrire au Service be-ys, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition de ses Utilisateurs.

Déclaration des Pratiques de Certification (DPC) : Document qui identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les PC qu'elle s'est engagée à respecter.

Infrastructure de Gestion de Clés (IGC) : Ensemble de composants, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance.

Liste des Certificats Révoqués (LCR) : 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.

One Time Password (OTP) : Code à usage unique qui permet à l'utilisateur de s'authentifier.

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 : Le porteur de certificat est la personne morale détentrice d'une bi-clé de signature cachet et identifiée directement ou indirectement (pseudonyme), dans le certificat de signature cachet.

Représentant Client (RC) : Personne physique qui est responsable de l'utilisation du Certificat de signature cachet pour le service identifié dans le Certificat et de la clé privée correspondant à ce Certificat, pour le compte du Client identifié dans ce Certificat. Le RC a un lien contractuel, hiérarchique et réglementaire avec le Client.

Service signature : Un des services de la gamme d'offres de services de dématérialisation et de confiance be-ys,

déployé en tout ou partie. Ici, il s'agit du Service de signature électronique be-ys.

Service d'horodatage : Ensemble des prestations nécessaires à la génération et à la gestion de Contremarques de temps.

Système d'horodatage : Ensemble des Unités d'horodatage et des composants d'administration et de supervision utilisés pour fournir des Services d'horodatage.

Signature électronique ou Signature : « Usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache », conformément à l'article 1367 du Code civil.

Unité d'Horodatage (UH) : Ensemble de matériel et de logiciel en charge de la création de Contremarques de temps caractérisé par un identifiant de l'Unité d'Horodatage accordé par une AC, et une clé unique de signature de Contremarques de temps.

3. CONTACT DE L'AUTORITE DE CERTIFICATION

Gouvernance IGC be-ys.

BE-INVEST International S.A.

be-invest – 17 rue Léon Laval –

L-3372 LEUDELANGE – Luxembourg

Email : gouvernance.igc@beys.com

4. TYPE DE CERTIFICATS EMIS

Les Certificats émis par l'AC « BE-YS CUSTOMER SERVICES CA NB » sont des Certificats de signature cachet délivrés aux RC.

Les Certificats sont émis à travers la chaîne de certification suivante :

AC Racine « ALMERYS ROOT CA »

|

AC « BE-YS CUSTOMER SERVICES CA NB »

Les Certificats de la chaîne de certification sont disponibles à l'adresse suivante : <http://pki.almerys.com>.

5. PRIX

Le prix correspondant à la fourniture du Certificat est intégré dans celui du Service de signature cachet électronique.

6. VALIDITE DES CGU

Les CGU sont valables à compter du premier jour de leur mise en ligne jusqu'au premier jour de la mise en ligne d'une nouvelle version.

Les Conditions générales qui s'appliquent sont celles dont la date de mise en ligne figure sur les présentes conditions générales.

Les présentes Conditions générales entrent en vigueur au moment de l'utilisation du Service de signature cachet électronique.

L'AC se réserve le droit de modifier à tout moment les présentes CGU notamment dans le cadre des évolutions législatives et réglementaires.

L'AC mettra en ligne chaque nouvelle version des CGU qui seront disponibles sur le site <http://pki.almerys.com> et informera le Client par courrier électronique et ou sur la page d'accueil du site de l'existence de cette nouvelle version et ce, trente (30) jours au minimum avant son application. En cas de désaccord avec les Nouvelles dispositions, le Client aura la faculté de résilier les CGU.

Les versions précédentes des CGU sont disponibles sur le site <http://pki.almerys.com>

7. MODALITES D'OBTENTION DU CERTIFICAT

Un RC peut obtenir un Certificat de signature Cachet Customers Services dans le cadre de la mise en œuvre du Service de signature cachet, ou d'horodatage.

Les demandes de Certificats nécessitent de fournir a minima les informations suivantes :

→ Identité du RC :

- o Prénom ;
- o Nom ;
- o Adresse mail ;

→ Organisation du Client :

- o Raison Sociale ;
- o Numéro SIREN pour les entreprises françaises, ou en dehors de la France, tout numéro d'identification équivalent reconnu par les autorités compétentes du pays du Client ;

o Extrait Kbis, ou de tout autre document d'identification équivalent reconnu par les autorités compétentes du pays du Client) permettant de justifier de l'existence de l'entreprise;

o Le nom à faire apparaître dans le champ CN du certificat (Application ou nom du Client pour un certificat cachet, ou nom de l'unité d'horodatage pour un certificat d'horodatage).

La génération de la Bi-clé et du Certificat a lieu en présence des équipes be-ys lors d'une Cérémonie des Clés (Key Ceremony) qui permet de s'assurer d'un niveau de protection important de la Bi-clé de Signature Cachet.

Une fois le Certificat produit, et la Signature Cachet par le Client du ou des document(s) présenté(s) à l'Utilisateur, le Certificat Cachet Customers Services est intégré dans le ou le(s) document(s) signé(s) et ou Horodaté(s) au format PDF. Ce(s) document(s) est (sont) ensuite mis à disposition du Client et de l'Utilisateur.

Les clés privées du Client sont générées et stockées à travers le Service de stockage sécurisé des clés. Des clés du Client lui sont dédiées et lui permettent exclusivement

d'apposer sa signature cachet sur ses documents.

En cas de présence du représentant légal ou du RC lors de la génération du Certificat, la signature du procès-verbal du Certificat vaut acceptation d'utilisation du Certificat.

En cas d'absence du représentant légal, et du RC, une notification par email est envoyée au RC de la génération du Certificat, avec le contenu du champ « sujet » du Certificat, la date d'émission et la date d'expiration. La non-contestation du Certificat par le RC dans les deux (2) semaines qui suivent la notification, ainsi que la première utilisation du Certificat par le Client vaut acceptation d'utilisation par le Client.

8. MODALITES DE RENOUELEMENT

Le Représentant Client est averti de l'arrivée à expiration de son Certificat par courriel deux (2) mois avant l'expiration.

La procédure de renouvellement mise en place par be-invest consiste à :

- Procéder à une demande de nouveau Certificat conformément au processus initial de Cérémonie des Clés.
- Détruire l'ancienne clé privée du Certificat précédent.

Lors d'une nouvelle demande de Certificat, l'opération de révocation du précédent est automatiquement réalisée par l'Autorité d'Enregistrement.

9. MODALITES DE REVOCATION

Révocation par le RC

La demande de révocation d'un certificat Client peut être faite :

- Par le RC qui remplit le formulaire de demande de révocation mis à sa disposition par l'AE ;

La révocation est effectuée par l'AE, qui valide ainsi la demande. La validation de la demande de révocation est opérée par l'AE qui :

- Contacte le RC ;
- Demande au RC de confirmer sa demande par mail ;
- Attend la confirmation du RC ;

Quand la demande est validée, le Certificat est alors

révoqué par l'Autorité d'Enregistrement.

Le demandeur de la révocation est tenu informé du bon déroulement de l'opération et de la révocation effective du Certificat.

Révocation suite au départ du RC

Le départ du RC de la structure du Client qui a effectué la demande initiale de Certificat n'est pas un motif de révocation d'un Certificat Client car le Certificat est attaché à un service du Client.

Le Client doit par ailleurs désigner un nouveau RC pour assurer la continuité de représentation du Client auprès de l'AE pour le certificat considéré.

Révocation suite à la fin de service

La fin de vie, naturelle ou anticipée, du contrat de Service entre le Client et l'AE, implique de fait la fin de la prestation d'hébergement sécurisé de la Bi-clé de signature cachet et la révocation du Certificat du Client.

Révocation d'urgence

La révocation d'urgence est possible en utilisant le service téléphonique des demandes de révocation disponible 24H/24 7j/7, tel qu'indiqué à l'adresse <http://pki.almerys.com/revoquer.html>

L'authentification des demandes de révocation s'effectue via un code OTP.

10. LIMITES D'USAGES

Les Certificats émis par l'AC « Customers Services CA

» ne sont utilisables qu'à des fins de signature cachet, dans le processus proposé par le Service de signature, ou d'horodatage be-ys mis à disposition de ses Clients et de leurs Utilisateurs.

Les Certificats sont émis pour une durée de trois (3) ans Maximum.

Ces Certificats ne sont pas utilisables :

- au-delà de leur période de validité ;
- pour signer des documents autres que ceux présentés dans le cadre du Service de signature, ou Service d'horodatage be-ys mis en œuvre pour le Client.

La liste des applications reconnues peut être demandée en écrivant au point de contact défini dans les présentes CGU.

11. OBLIGATIONS DES CLIENTS, DES REPRESENTANTS CLIENTS

Les Représentants Clients sont responsables de la véracité des informations personnelles et des informations du Client qu'ils fournissent dans le cadre de leur relation avec l'AE. En particulier des données suivantes :

- Prénom et Nom,
- Adresse de courrier électronique (mail),
- Numéro SIREN /SIRET pour les entreprises françaises, ou en dehors de la France, tout numéro d'identification équivalent reconnu par les autorités compétentes du pays du Client,
- Raison sociale du Client.

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

Le Représentant Client a le devoir :

- de vérifier l'exactitude des informations qu'il a fournies et qui lui sont présentées lors de la KC ;
- le cas échéant, d'informer l'AE de toute modification concernant ses informations personnelles ;
- d'accepter les CGU qui lui sont présentées pour l'acceptation du Certificat ;
- de n'utiliser les Certificats délivrés par « BE-YS CUSTOMER SERVICES CA NB » qu'à des fins de signature cachet, conformément à la PC de l'AC « BE-YS CUSTOMER SERVICES CA NB » à l'adresse suivante :

<http://pki.almerys.com/intermediate/be-yscustomerservicescanb/certificatePolicy/PKA013B%20-%20PC-Customers%20Services%20CA%20NB.pdf>

et aux présentes CGU ;

- de protéger les données sensibles qui pourront lui être remises à l'issue de la KC, à lui ainsi qu'à d'autres personnes qu'il a désignées.

12. OBLIGATIONS DE VERIFICATION DES CERTIFICATS PAR LES APPLICATIONS UTILISATRICES

Les Applications utilisatrices des certificats doivent :

- vérifier l'usage pour lequel le Certificat a été émis ;

→ vérifier que le Certificat utilisé a bien été émis par l'AC « BE-YS CUSTOMER SERVICES CA NB » ;

→ vérifier l'accès à la liste des Certificats révoqués (LCR) de l'AC « BE-YS CUSTOMER SERVICES CA NB » ;

→ Vérifier la signature du Certificat, et de la chaîne de certification, jusqu'à l'AC Racine « ALMERYS ROOT CA » et contrôler la validité des Certificats au regard des LCR des différentes AC.

Les Certificats de la chaîne de confiance et les LCR de l'AC « BE-YS CUSTOMER SERVICES CA NB » et de l'AC « ALMERYS ROOT CA » sont disponibles à l'adresse suivante : <http://pki.almerys.com>

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

Ces informations sont disponibles 24h/24.

13. OBLIGATION DE L'AC

L'AC « Customers Services CA NB » be-ys est expressément tenue à une obligation de moyens pour toutes les obligations relatives à la gestion du cycle de vie du Certificat qu'elle émet.

14. LIMITE DE RESPONSABILITE DE L'AC

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

L'AC « BE-YS CUSTOMER SERVICES CA NB » décline en particulier sa responsabilité pour tout dommage résultant :

→ d'un emploi des Bi-clés pour un usage autre que ceux prévus avec le Client ;

→ de l'usage de Certificats expirés ;

→ d'un cas de force majeure reconnu par les cours et tribunaux de l'Etat du siège du Porteur.

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

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

15. DONNEES A CARACTERE PERSONNEL, ET CONSERVATION DES DONNEES

Les traitements de Données à caractère personnel effectués dans le cadre des présentes CGU, devront intervenir en conformité avec les dispositions du Règlement (UE) 2016/679 – le « RGPD » entré en application le 25 mai 2018, ainsi que toute autre loi ou réglementation applicable aux traitements en matière de protection des données à caractère personnel en vigueur avant le 25 mai 2018 (ci-après ensemble : la « Réglementation Applicable ») ou tout nouveau texte applicable qui viendrait remplacer ces textes.

En qualité de responsable de traitement, be-invest utilise les données personnelles exclusivement pour l'exécution des présentes

CGU. La finalité du traitement est la gestion du cycle de vie des Certificats des Porteurs (émission, révocation, et renouvellement), et le cas échéant, la relation commerciale, et la facturation du service. Conformément au RGPD, Le Porteur dispose du droit de demander l'accès, la rectification, l'effacement (sous réserve des disposition eIDAS) ou la limitation du traitement le concernant, ou de s'opposer au traitement pour un motif légitime, ainsi que de demander la portabilité de ses données.

Pour toutes questions, réclamations ou pour faire valoir ses droits, le Porteur peut contacter le Délégué à la Protection des Données :

Soit par voie électronique : dpo@be-ys.com

Soit par voie postale à l'adresse suivante :

BE-INVEST International S.A.

17 rue Léon Laval

L-3372 LEUDELANGE LUXEMBOURG

Les données personnelles collectées par les Autorités d'Enregistrement, sont conservées ainsi que les journaux d'évènement au maximum dix années après expiration des Certificats.

16. REFERENCES DOCUMENTAIRES

La PC de « BE-YS CUSTOMER SERVICES CA NB » pour les Certificats de signature est accessible à l'adresse suivante :

<http://pki.almerys.com>

L'OID de cette Politique est

1.3.6.1.4.1.48620.41.1.5.2.1.

Les OID des certificats sont :

- de personne morale (OID 1.3.6.1.4.1.48620.41.1.5.2.2.1.1) ETSI EN 319411-1 LCP

- cachet d'horodatage (OID

1.3.6.1.4.1.48620.41.1.5.2.2.2.1) ETSI EN 319411-1 LCP

17. INTEGRALITE DES CGU

Les présentes CGU du service de signature cachet électronique constituent l'intégralité des accords entre les Parties en ce qui concerne la réalisation de l'objet des présentes, et annulent et remplacent tous accords et propositions antérieurs ayant le même objet quelle qu'en soit la forme.

18. REGLEMENT DES LITIGES ET LOI APPLICABLE

A défaut de solution amiable, et dès lors que le siège social du Porteur du certificat électronique est situé en France, tout différend pouvant naître à propos de la validité, de l'interprétation, de l'exécution ou, plus généralement, des présentes CGU sera soumis à la loi française ainsi qu'à la compétence des juridictions françaises.

Si le siège social du Porteur du certificat électronique n'est pas situé en France, tout différend pouvant naître à propos de la validité, de l'interprétation, de l'exécution ou, plus généralement, des présentes CGU sera soumis à la loi luxembourgeoise ainsi qu'à la compétence des juridictions luxembourgeoises.

Pour toute demande d'information ou réclamation relative au service Certificats de signature cachet, il convient dans un premier temps de contacter le service Autorité de Certification par mail à l'adresse suivante : gouvernance.igc@be-ys.com, et ce, avant même les étapes de conciliation et la saisie éventuelle des tribunaux compétents.

Les Parties s'efforceront de régler à l'amiable tout litige concernant l'interprétation ou l'exécution du contrat dans les meilleurs délais.

19. AUDITS ET REFERENCES APPLICABLES

Un contrôle de conformité de l'AC « BE-YS CUSTOMER SERVICES CA NB » à la PC et à la DPC qui lui sont applicables pourra être effectué, sur demande de l'Autorité de Gouvernance de l'IGC be-ys.

L'AG s'engage à effectuer ce contrôle au minimum une fois tous les 3 ans.

D'autre part, dans le cadre de la certification ETSI 319411-1, un audit de maintien de conformité sera réalisé annuellement par une société accréditée à partir de la date d'obtention de la certification.

Nom, Prénom :

Date, Signature et cachet d'entreprise :