1. OBJET DES CGU

Les présentes Conditions Générales d'Utilisation (ci-après dénommées « CGU ») ont pour objet de préciser le contenu et les modalités d'utilisation des Certificats de signature délivrés par l'AC « ALMERYS USER SIGNING CA NB» d'almerys ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les Certificats User Signing sont utilisés dans le cadre du déploiement du Service de signature électronique en ligne proposé par almerys à ses Clients et à leurs Utilisateurs.

Les Certificats émis par l'AC «ALMERYS USER SIGNING CA NB» sont des Certificats à usage unique à destination de Porteurs, personnes physiques, qui sont les Utilisateurs du Service de signature électronique mis en œuvre par Almerys pour ses Clients.

L'activation de la Bi-clé associé à un Certificat de signature permet la signature des informations et documents du Client présentés au Porteur par le Service de signature électronique.

2. DEFINITIONS

Applications utilisatrices : Services applicatifs exploitant les Certificats émis par l'AC « User Signing CA », par exemple, pour des besoins de vérification de signature du Porteur.

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 Almerys avec pouvoir décisionnaire.

Bi-clé : Couple clé publique/ clé privée

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 almerys, qu'elle utilise pour ses propres besoins ou qu'elle met à disposition des 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.

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 certificat ne peut être qu'une personne physique. Il s'agit de l'Utilisateur du Service de signature électronique d'Almerys qui doit respecter les conditions qui lui incombent définies dans la PC de l'AC « User Signing CA » et dans les présentes CGU. Le porteur de certificat est nominativement identifié dans le certificat électronique qui lui est délivré par l'AC

Service : Un des services de la gamme d'offres de services de dématérialisation et de confiance d'Almerys, déployé en tout ou partie. Ici, il s'agit du Service de signature électronique Almerys.

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

3. CONTACT DE L'AUTORITE DE CERTIFICATION

Gouvernance IGC

Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9
gouvernance.igc@be-ys.com

4. TYPE DE CERTIFICATS EMIS

Les Certificats émis par l'AC « ALMERYS USER SIGNING CA NB» sont des Certificats de signature électronique délivrés aux Porteurs, Utilisateurs du Service de signature almerys. Les certificats délivrés sont utilisés par le porteur pour la signature de son contrat. La durée de vie de ce certificat est alors éphémère, valable uniquement pour cette opération.

Les clés privées des porteurs sont générées et stockées par almerys pour la durée de la transaction. almerys utilise un matériel cryptographique pour assurer le niveau de sécurité de cette opération.

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

AC Racine « ALMERYS ROOT CA »

|

AC « ALMERYS USER SIGNING CA NB»

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

5. PRIX

Sans objet car la fourniture du Certificat à usage unique est intégrée dans le Service de signature électronique almerys.

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 de la nouvelle version des CGU.

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 électronique.

Les Conditions Générales d'Utilisation du certificat sont intégrées aux Conditions Générales du Service de signature et elles sont acceptées par le Porteur au moment de la signature de son contrat.

Si les Conditions Générales d'Utilisation du Certificat sont amenées à être modifiées, le Porteur acceptera la nouvelle version au moment de la délivrance d'un nouveau certificat, c'est à dire au moment de la signature d'un nouveau contrat.

En cas de refus des CGU par le Porteur, le certificat n'est pas généré et la transaction de signature annulée.

7. MODALITES D'OBTENTION ET D'ACTIVATION DU CERTIFICAT

Un Porteur peut obtenir un Certificat de signature User Signing 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 de signature, établie à l'issue d'une phase d'identification à 2 facteurs. Cette identification se base par défaut sur :
    - La fourniture par mail d'une URL unique personnalisée de signature au Porteur ;
    - L'envoi d'un code à usage unique (One Time Password) 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 une Bi-clé pour ce Porteur et pour cette session. Cette

Bi-clé est protégée matériellement dans un Module cryptographique matériel hébergé dans les locaux sécurisés d'Almerys, conforme au minimum au standard FIPS 140-2 level 2.

- L'authentification réussie de la session permet l'activation de la clé privée pour l'action de Signature.

L'acceptation du contenu du Certificat est explicite et se fait en ligne après acceptation des présentes CGU et avant utilisation du Certificat pour signature des documents présentés par le Client.

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

- Identité du Porteur :
  - Prénom ;
  - Nom ;
- Organisation du Client :
  - Raison Sociale ;
  - n° SIREN ou équivalent;
- Un Identifiant de transaction unique et aléatoire associé de manière univoque à une session de signature propre au Porteur.

Les données permettant de générer la demande de Certificat sont scellées par almerys et ne peuvent être modifiées durant la session de signature.
La seule modification autorisée avant l'établissement du Certificat est la troncature des nom et prénom du Porteur si ceux-ci sont excessivement longs.

Une fois le Certificat produit, et la Signature du ou des documents présentés au Porteur effective, le Certificat User Signing est intégré dans le ou les documents signés au format PDF qui sont mis à disposition du Porteur et du Client.

8. MODALITES DE RENOUVELLEMENT

Les Certificats ne sont pas renouvelables étant donné qu'ils ne sont utilisés qu'une fois dans le cadre d'une transaction de signature.

Si une nouvelle transaction de signature est initiée pour un même Porteur, cela nécessite l'émission d'un nouveau Certificat qui contiendra un nouvel identifiant de transaction.

9. MODALITES DE REVOCATION

Le Certificat de signature User Signing a une durée de vie égale à 24 (vingt-quatre) heures.
Etant donné cette courte durée de vie des Certificats de signature, et leur cadre d'usage unique, seule la non acceptation du Certificat par l'Utilisateur, au cours du processus de signature, active la fonction de révocation. Cette révocation a pour conséquence la fin de la transaction de signature courante et la redirection du Porteur vers la page d'accueil du Service de signature électronique.

D'autre part, la Bi-clé de signature ne pouvant être activée qu'une fois dans le cadre d'une transaction de signature, il est détruit à l'issue de la transaction considérée, quel que soit le statut final de la transaction.

10. LIMITES D'USAGES

Les Certificats émis par l'AC «ALMERYS USER SIGNING CA NB» ne sont utilisables qu'à des fins de signature, dans le processus proposé par le Service de signature almerys mis à disposition de ses Clients et de leurs Utilisateurs.

Les Certificats sont à usage unique dans le cadre d'une session de signature.

Ces Certificats ne sont pas utilisables :

- au-delà de leur période de validité ;
- pour signer des documents autres que ceux présentés au Porteur dans le cadre du Service de signature Almerys mis en œuvre pour le Client.

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

11. OBLIGATIONS DES PORTEURS

Les Porteurs de certificat sont responsables de la véracité des informations personnelles qu'ils ont fournies dans le cadre de leur relation avec le Client. En particulier, on considère les données suivantes :

- Prénom et Nom,
- Adresse de courrier électronique (*mail*),
- Numéro de téléphone portable.

Dans tous les cas, le Client est responsable du maintien à jour les informations du Porteur.

Le Porteur a le devoir de :

- vérifier l'exactitude des informations personnelles qu'il a fournies et qui lui sont présentées dans la session de signature en ligne ;
- le cas échéant, d'informer le Client de toute modification concernant ses informations personnelles ;
- accepter les CGU via l'activation d'une case à cocher présentée dans le processus de signature ;
- n'utiliser les Certificats délivrés par «ALMERYS USER SIGNING CA NB» qu'à des fins de signature, conformément à la PC de l'AC « User Signing CA NB» et aux présentes CGU ;
- protéger les données d'identification qui valident l'activation de la session de signature et l'acte de génération de la Bi-clé et du Certificat de signature, en particulier assurer la non divulgation du mot de passe de sa boîte mail et le non partage du téléphone portable sur lequel est reçu le code à usage unique (OTP).

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 «ALMERYS USER SIGNING CA NB» ;
- vérifier l'accès à la liste des certificats révoqués (LCR) de l'AC «ALMERYS USER SIGNING 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 «ALMERYS USER SIGNING CA NB» et de l'AC « ALMERYS ROOT CA » sont disponibles à l'adresse suivante : http://pki.almerys.com

13. OBLIGATION DE L'AC

L'AC « ALMERYS USER SIGNING CA NB» d'Almerys 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 « ALMERYS USER SIGNING CA NB» d'almerys 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 « ALMERYS USER SIGNING CA NB» d'almerys 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 tel que défini par les tribunaux français.

L'AC « ALMERYS USER SIGNING CA NB» d'almerys décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.

En aucun cas, l'AC « ALMERYS USER SIGNING 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 via le Service de signature électronique d'almerys.

15. DONNEES A CARACTERE PERSONNEL

Le Porteur reconnait, via la demande de certificat, avoir consenti au traitement de ses données pour la gestion de son certificat de signature, la conservation

et le traitement de ses données, conformément au Règlement Général sur la Protection des Données (RGPD). En particulier, Le Porteur dispose du droit de demander la rectification, l'effacement 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 :

46, rue du ressort,

63967 CLERMONT-FERRAND CEDEX 9

16. REFERENCES DOCUMENTAIRES

La PC de «ALMERYS USER SIGNING CA NB» pour les Certificats de signature à usage unique est accessible à l'adresse suivante :

http://pki.almerys.com

L'OID de cette Politique est 1.3.6.1.4.1.48620.41.1.4.2.1.
Les OID des certificats sont :

- l'OID 1.2.250.1.16.12.5.41.1.4.2.1.1 pour les certificats ETSI 102042 LCP
- l'OID 1.3.6.1.4.1.48620.41.1.4.2.1.1.1 pour les certificats ETSI EN 319411 LCP,

17. INTEGRALITE DES CGU

Les parties reconnaissent que les présentes Conditions Générales, les CGU du service de signature électronique constituent l'intégralité des accords entre elles 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

Les présentes CGU sont soumises au droit français.

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.

Les parties s'efforceront de régler à l'amiable tout litige concernant l'interpretation ou l'exécution du contrat dans les meilleurs délais. En l'absence de conciliation tout litige relatif à la validité, l'interprétation ou l'exécution des présentes CGU sera soumis aux tribunaux compétents de Clermont-Ferrand.

19. AUDITS ET REFERENCES APPLICABLES

Un contrôle de conformité de l'AC « ALMERYS USER SIGNING 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 almerys.

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 319401 and ETSI 319411, un audit de maintien de conformité sera réalisé annuellement par la société accréditée LSTI à partir de la date d'obtention de la certification.