Autorité de Certification SIGNATURE AND AUTHENTICATION CA NC : Conditions Générales d'Utilisation des certificats personnes physiques

version v1.7, 19/04/2018, Réf. : MPKIG044, diffusion publique

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 cachet qualifié, de signature à distance de signature qualifiée, d'unité d'horodatage et d'authentification délivrés par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » d'Almerys ainsi que les engagements et obligations respectifs des différents acteurs concernés.

Les Certificats « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » sont utilisés dans le cadre du déploiement des Services de dématérialisation proposés par almerys ou par les partenaires almerys à ses Clients et à leurs Utilisateurs.

Les Certificats de signature et d'authentification, ainsi que les certificats de signature à distance émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC »sont des Certificats à destination des Clients, personnes physiques qui sont des clients du Services de dématérialisation qu'almerys met en œuvre pour eux.

Les Certificats de cachet émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » sont des Certificats à destination des Clients, personnes morales, leur permettant de sceller des documents et message afin d'en garantir l'origine et l'intégrité.

Les Certificats d'unité d'horodatage émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » sont des Certificats à destination des unités d'horodatage d'almerys, utilisés dans le cadre du service d'horodatage qualifié mis en place par Almerys.

Les Bi-clés de signature qualifiée et d'authentification sont générées de manière sécurisée dans un module cryptographique « carte à puce » répondant aux exigences d'un SSCD éligible pour la signature qualifiée ETSI 101456 ou ETSI 319411-2.

Les certificats de signature à distance, de cachet et d'unité d'horodatage sont générés et utilisés dans un service de gestion de clé à distance et opéré de façon sécurisée par almerys

2. DEFINITIONS

Abonné : souscripteur au service de certification électronique, qui peut être le porteur dans le cas d'un certificat pour un particulier, ou d'une personne physique agissant pour une personne morale dans le cadre d'un certificat entreprise notamment.

Applications utilisatrices : Services applicatifs exploitant les Certificats émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC », par exemple, pour des besoins de vérification de signature.

Autorité d'Enregistrement (AE): autorité en charge de vérifier l'identité et la qualité d'un demandeur de certificat, de la personnalisation des cartes, et de la remise en main propre au Porteur. La fonction d'AE est remplie soit par le :

- Personnels d'almerys,
- Personnels d'un client almerys auxquels l'AC almerys a délégué la fonction d'autorité d'enregistrement.

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

Cérémonie des Clés ou Key Ceremony (KC) : Réunion spéciale des personnes autorisées pour générer le certificat d'AC. 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 Almerys, 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 (SSCD): 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 : personne physique titulaire du certificat.

Service signature : 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.

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

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 be-ys

Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9

Téléphone : 04 73 74 82 98

gouvernance.igc@be-ys.com

4. TYPE DE CERTIFICATS EMIS

Les Certificats émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » sont

- Des Certificats de signature et d'authentification personne physique.
- Des Certificats de signature à distance
- Des certificats de cachet et d'unité d'horodatage

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

AC Racine « ALMERYS ROOT CA »

|

AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC»

Les Certificats de la chaîne de certification sont disponibles à l'adresse suivante :

http://pki.almerys.com.

5. PRIX

Le coût du SERVICE dépend des prestations fournies, il est communiqué par l'AE au porteur (abonné).

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 offre.

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 des certificats.

Ces CGU sont disponibles sur le site http://pki.almerys.com

7. MODALITES D'OBTENTION DU CERTIFICAT

L'émission du certificat du Porteur est faite par les Autorités d'Enregistrement de l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC »au travers de l'infrastructure technique. L'AE se charge de réunir et de vérifier les informations nécessaires à l'obtention du certificat.

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

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

- Le lieu de naissance du Porteur ;
- La date de naissance du Porteur ;
- Une adresse postale et/ou une adresse email et/ou un numéro de téléphone portable.
- Le dossier de demande ainsi que les présentes CGU devront être signés par le Porteur

Dans le cas d'un certificat « entreprise », d'un certificat « cachet » ou d'un certificat d'unité d'horodatage, le demandeur devra fournir en supplément :

- Une pièce, valide lors de la demande de certificat (extrait Kbis ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Établissements ou inscription au répertoire des métiers, ...), attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci.
- Optionnellement un justificatif du titre ou attribut du porteur,
- Le dossier de demande devra être co-signé par le représentant légal de l'entreprise

Pour les certificats de signature qualifiée et d'authentification, les clés privées du porteur sont générées et stockées dans un SSCD qui lui est remis en main propre. Ce SSCD sera personnalisé par l'AE en présence du Porteur.

Lors de la remise du support au Porteur, ce dernier doit signer un procès-verbal de réception du support cryptographique qui constitue son acceptation explicite du certificat.

Dans le cas d'un certificat de cachet ou d'unité d'horodatage, le bi-clé est généré dans un service de signature sécurisé durant une cérémonie des clés. La remise du certificat et de la copie du script de cérémonie constitue l'acceptation du certificat.

Dans le cas d'un certificat de signature à distance, le téléchargement du certificat ou d'un message contenant le certificat constitue une acceptation implicite de celui-ci.

8. MODALITES DE RENOUVELLEMENT

Le Porteur est averti de l'arrivée à expiration de son certificat par courriel 2 mois avant l'expiration.

La procédure de renouvellement mise en place par almerys consiste à :

- Procéder à une demande de nouveau certificat conformément au processus initial.
- Détruire l'ancien support SSCD or QSCD qui lui a été remis, dans le cas d'un certificat de signature qualifié ou d'authentification.

9. MODALITES DE REVOCATION

Le Porteur ne peut pas accéder aux services de révocation directement. Lorsqu'il souhaite procéder à la révocation de son certificat, il doit soit :

- Contacter l'Autorité d'Enregistrement en se rendant auprès de son agence, ou par téléphone. Dans ce cas l'Autorité d'Enregistrement identifiera le Porteur si elle en a les moyens ou bien révoquera d'elle – même le certificat concerné;
- Contacter le centre de support identifié par le Client correspondant, ou le support almerys par téléphone : 0 825 306 015 (horaires : 9h-12h / 13h30-17h30). Dans ce cas le centre de support procèdera à l'identification du Porteur, s'il en a les moyens révoquera le certificat, ou bien transmettra la demande à l'Autorité d'Enregistrement correspondante;
- Utiliser le service d'enregistrement des demandes de révocation disponible en ligne 24H/24 7j/7, à l'adresse http://pki.almerys.com/revoquer.html , l'authentification des demandes de révocation s'effectue via un code OTP.

Dans tous les cas, l'AC ou l'AG ont toute latitude pour procéder à la révocation d'un certificat final émis par l'AC.

10. LIMITES D'USAGES

Les Certificats émis par l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » ne sont utilisables qu'à des fins de signature, de cachet et ou d'authentification selon leur usage respectif.

Les Certificats sont émis pour une durée maximale de 3 ans.

Ces Certificats ne sont pas utilisables au-delà de leur période de validité ;

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 (ABONNES)

Les Porteurs de certificats sont responsables de la véracité des informations qu'ils fournissent dans le cadre de leur relation avec almerys. Ils doivent notamment :

- communiquer des informations exactes et à jour lors de la demande ou du renouvellement du Certificat,
- rencontrer en face à face l'Autorité d'Enregistrement pour procéder à la vérification de ses informations d'identité,
- gérer de manière sécurisée les secrets et éléments sensibles qui lui sont remis à l'issue de la procédure de génération de son certificat En particulier le porteur particulier doit garder sa clé privée sous son contrôle exclusif.
- accepter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- informer l'AE de toute modification concernant les informations contenues dans son Certificat,
- faire, sans délai, une demande de révocation de son Certificat auprès de l'AE en cas de perte, ou de suspicion de compromission de sa clé privée (ou de ses données d'activation).

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 SIGNATURE AND AUTHENTICATION CA NC » ;
- vérifier l'accès à la liste des certificats révoqués (LCR) de l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » ;
- 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 SIGNATURE AND AUTHENTICATION CA NC » 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. LIMITE DE RESPONSABILITE DE L'AC

Sous réserve des dispositions d'ordre public applicables, l'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » 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 SIGNATURE AND AUTHENTICATION CA NC » 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 l'article 1218 du Code civil.

L'AC « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » 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.

14. DONNEES A CARACTERE PERSONNEL, ET CONSERVATION DES DONNEES

Le Porteur reconnait, via la signature de la demande de certificat, avoir consenti au traitement de ses données pour la gestion de ses certificats de signature et d'authentification, 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

15. REFERENCES DOCUMENTAIRES

La PC de « ALMERYS SIGNATURE AND AUTHENTICATION CA NC » pour les Certificats de signature est accessible à l'adresse suivante :

http://pki.almerys.com

L'OID de cette Politique est : 1.2.250.1.16.12.5.41.1.7.3.1.

Les OID des certificats sont :

- OID = 1.2.250.1.16.12.5.41.1.7.3.1.1.1 : pour les certificats de signature qualifiés ETSI 101456 QCP public+SSCD (directive européenne 1999/93/EC),
- OID = 1.2.250.1.16.12.5.41.1.7.3.1.2.1 : pour les certificats d'authentification ETSI 102042 NCP+,
- OID =1.3.6.1.4.1.48620.41.1.7.3.1.1.1: pour les certificats de signature qualifiés ETSI EN 319411-2 (conforme au Règlement Européen eIDAS)
- OID = 1.3.6.1.4.1.48620.41.1.7.3.1.2.1: pour les certificats d'authentification ETSI 319411-1 NCP+
- OID = 1.3.6.1.4.1.48620.41.1.7.3.1.4.1 pour les certificats cachet qualifiés ETSI EN 319411-2 (conforme au Règlement Européen eIDAS)
- OID 1.3.6.1.4.1.48620.41.1.7.3.1.5.1 pour les certificats cachet horodatage qualifiés ETSI EN 319411-2 (conforme au Règlement Européen eIDAS)
- OID=1.3.6.1.4.1.48620.41.1.7.3.1.3.1 pour les certificats qualifiés de signature à distance ETSI EN 319411-2 QCP (conforme au Règlement Européen eIDAS)

16. INTEGRALITE DES CGU

Les parties reconnaissent que les présentes conditions générales, les CGU des services 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.

17. COUVERTURE D'ASSURANCE

almerys déclare être assuré auprès d'une compagnie notoirement solvable en responsabilité civile couvrant les prestations des services de certification électronique.

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 SIGNATURE AND AUTHENTICATION CA NC, 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'interprétation 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 SIGNATURE AND AUTHENTICATION CA NC » 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 ETSI 319411, un audit de certification et de maintien de conformité sera réalisé annuellement par la société accréditée LSTI à partir de la date d'obtention de la certification.

NOM Prénom

Date, Signature du porteur