

# CONDITIONS GENERALES D'UTILISATION DU SERVICE DE CONTRACTUALISATION EN LIGNE

Orange propose un service de contractualisation en ligne (ci-après le « **Service de contractualisation en ligne** »), qui permet à ses clients (ci-après individuellement désignés l'« **Utilisateur** ») de souscrire en ligne des services fournis par Orange, dans un contexte informatiquement et légalement sécurisé.

Pour permettre à l'Utilisateur de souscrire en ligne les services fournis par Orange dans le cadre du Service de contractualisation en ligne, Orange s'appuie sur Almerys, prestataire de services de certification électronique répondant aux normes légales et réglementaires.

## Article 1 – Définitions

**Almerys** : société par actions simplifiée au capital de 40 000 euros, inscrite au Registre du commerce et des sociétés de Clermont-Ferrand sous le numéro B 432 701 639, ayant son siège social 46 rue du ressort – 36100 Clermont-Ferrand.

**Certificat** : désigne un fichier électronique attestant qu'une bi-clé appartient à l'Utilisateur, directement ou indirectement (pseudonyme).

**Données à caractère personnel** : désigne l'ensemble des données transmises par l'Utilisateur en vue de leur traitement dans le cadre de l'utilisation du service de contractualisation en ligne.

**Dossier de preuve** : désigne l'ensemble des éléments collectés par Orange dans le cadre du processus de contractualisation entre l'Utilisateur, **Orange**, puis conservés par **Orange**, pendant un délai de dix (10) ans, permettant ainsi d'assurer la traçabilité de la souscription.

**Identifiant** : désigne le pseudonyme choisi par l'Utilisateur lors de son inscription sur le site Sosh ou Orange et utilisé ensuite par l'Utilisateur pour accéder à son compte.

**Jeton d'horodatage** : désigne la donnée signée qui lie une représentation d'une donnée à un temps particulier, exprimée en heure UTC (Temps universel coordonnée), établissant ainsi la preuve que la donnée existait à cet instant-là.

**Mot de passe** : désigne le code personnel, exclusif et confidentiel qui, associé à l'Identifiant, est demandé à l'Utilisateur pour accéder à son compte.

**Orange** : société anonyme immatriculée au Registre du commerce et des sociétés de Paris sous le numéro 380 129 866 et **commercialisant les marques Orange et Sosh**.

**Service de contractualisation en ligne** : désigne le présent service proposé par **Orange** et mis en œuvre par Almerys visant à proposer une souscription fondée sur la signature électronique, à l'utilisateur.

**Signature électronique** : désigne l'usage d'un procédé fiable d'identification garantissant le lien entre la signature électronique et l'acte auquel elle s'attache, conformément à l'article 1316-4 du Code civil.

**Transaction de signature** : désigne l'ensemble d'échanges entre les parties dans le cadre du Service de contractualisation en ligne (Utilisateur, **Orange**, Almerys) dont le but est de permettre aux parties de s'engager sur un ensemble de documents contractuels. Elle comprend la signature des documents par l'Utilisateur, l'insertion d'un Jeton d'horodatage dans chacune de ces signatures, la gestion des phases d'authentification ou de sur-authentification, et la création d'un Dossier de preuve.

**Utilisateur** : désigne la personne qui souhaite souscrire une offre contractuelle Orange proposée.

## Article 2 – Objet

Les présentes Conditions générales d'utilisation ont pour objet de définir les étapes du Service de contractualisation en ligne permettant la signature en ligne des documents contractuels proposés par **Orange**, ainsi que les droits et obligations des parties dans le processus de contractualisation, d'archivage et de preuve desdits documents contractuels.

## Article 3 – Nature

Dans la mesure où le contrat conditionne la signature électronique par les parties de chacun des documents contractuels afférents à une offre d'Orange, les présentes Conditions générales d'utilisation du Service de contractualisation en ligne doivent être obligatoirement acceptées préalablement à chaque processus de contractualisation.

## Article 4 – Procédure d'information, de souscription et de signature du contrat

### **4.1. Procédure d'information et de conseil en ligne**

**Orange** met à disposition les documents contractuels applicables aux offres proposées à l'Utilisateur, d'une manière qui permette leur

conservation. Orange pourra sur demande du client transmettre les mandats SEPA ayant fait l'objet d'une signature électronique.

#### 4.2. Procédure de souscription du contrat en ligne

Pour souscrire le contrat par voie électronique l'Utilisateur doit manifester son acceptation de l'offre qui lui est proposée par **Orange**, en se conformant aux différentes étapes suivantes :

- avant la conclusion du contrat, communiquer avec précision à **Orange**, les informations nécessaires pour que les documents contractuels puissent être préparés en vue de la procédure de contractualisation par voie électronique,
- avant la conclusion du contrat, relire les rubriques et documents qu'il aura renseignés, le détail et le coût total de l'offre, identifier les erreurs commises dans la saisie des données et les corriger
- apposer sa signature électronique à l'aide de la clé de signature, dans les conditions ci-dessous décrites.

En acceptant les présentes Conditions générales d'utilisation du Service de contractualisation en ligne, l'Utilisateur atteste :

- avoir pris connaissance et approuvé sans réserve les documents contractuels qui lui sont soumis dans le cadre du Service de contractualisation en ligne,
- être dûment habilité aux fins de signature de ces documents contractuels.

L'ensemble des données fournies au moment de la souscription est sécurisé par la technologie d'Almerys.

Une fois les étapes contractuelles validées, l'utilisateur doit impérativement imprimer le contrat et ses accessoires (formulaire, grille tarifaire, etc.) ou les télécharger pour conservation.

#### 4.3. Procédure de signature en ligne

**Orange** propose à l'Utilisateur de formaliser son consentement dans le cadre du Service de contractualisation en ligne à l'aide d'une signature électronique.

**Orange** a choisi Almerys, prestataire de services de gestion de preuve, pour fournir à ses clients un service permettant de proposer la conclusion des contrats sous forme électronique, au moyen d'une signature électronique associée à un certificat avec une durée de vie limitée à quelques minutes, émis pour chaque contrat, et de constituer pour archivage électronique un Dossier de preuve relatif au contrat conclu en ligne. Le Dossier de preuve est généré à la suite de la dernière signature, apposée

par **l'utilisateur**. Le Dossier de preuve créé permet de garantir l'intégrité des documents contractuels ainsi que le lien existant entre l'Utilisateur et les documents contractuels auxquels il aura souscrits, et ce pendant la durée contractuellement prévue. Il contient l'ensemble des éléments techniques ayant concouru à la conclusion du contrat.

Le procédé mis en œuvre permet :

- la signature d'actes originaux par différentes parties,
- l'horodatage des actes originaux,
- la création et la transmission d'un Dossier de preuve.

La signature électronique proposée sur les sites Orange et Sosh est un procédé technique sécurisé permettant d'assurer l'identification des signataires, l'intégrité du document et de manifester le consentement du signataire aux documents signés.

La signature électronique permet ainsi d'établir un lien entre ces trois éléments et de garantir l'authenticité et l'intégrité de l'ensemble des informations fournies à l'Utilisateur, et notamment des documents contractuels.

Les documents sont présentés sous format PDF. La signature porte sur l'ensemble des documents suivants, à savoir notamment :

- Mandat SEPA Orange
- Mandat SEPA Orange Lease le cas échéant (pour les offres Sosh)

Les étapes de la signature électronique sont les suivantes :

- l'Utilisateur se connecte sur le site Orange ou Sosh
- l'Utilisateur fournit les informations demandées pour renseigner les rubriques et documents requis : civilité, nom, prénom, coordonnées (adresse, email, numéro de mobile le cas échéant)
- l'Utilisateur valide les conditions contractuelles d'Orange
- l'Utilisateur saisit ses coordonnées bancaires
- les coordonnées de l'Utilisateur sont vérifiées par envoi d'un SMS ou d'un email, d'un code d'authentification, à usage unique, composé de huit caractères, valable cinq (5) minutes, qui sert à authentifier la signature en ligne de l'Utilisateur,
- l'Utilisateur saisit le code d'authentification reçu (Etape 2). Si au bout de trois tentatives, il n'a pas saisi la bonne clé d'authentification, s'il a généré trois codes sans pouvoir

s'authentifier, le processus de signature est terminé. La dématérialisation du mandat SEPA ne sera plus possible et le client devra passer en procédure papier pour sa souscription en cours.

- L'Utilisateur consulte le mandat
- L'Utilisateur valide le contenu des documents qui lui sont présentés de manière intégrale ; l'application oblige l'Utilisateur à visualiser l'intégralité des onglets sur lesquels le contrat et ses accessoires sont présentés,
- si l'Utilisateur est d'accord sur les termes du contrat et de ses conditions (générales, spécifiques, particulières), il coche la case pour accepter préalablement les conditions générales du service et indiquer qu'il a bien pris connaissance des documents (Etape 3),
- l'Utilisateur peut alors cliquer sur « Signer électroniquement et autoriser le prélèvement ». Après avoir cliqué sur le bouton « valider » de l'étape de saisie de son code d'authentification, le client pourra télécharger le certificat de signature en cliquant sur le lien présent sur la fenêtre. L'Utilisateur a cinq minutes pour déclencher le processus de signature,
- l'Utilisateur procède à la signature du ou des mandat(s) et de ses accessoires en ligne en cliquant sur le bouton « Signer électroniquement et autoriser le prélèvement » ; après avoir cliqué sur « Signer électroniquement et autoriser le prélèvement », le ou les mandat(s) et ses accessoires sont signés ;
- une page de confirmation est alors présentée pour indiquer le succès ou l'échec de la transaction,
- Le mandat signé sera téléchargeable à partir de l'écran suivant ; Si l'utilisateur le souhaite, son ou ses mandat(s) SEPA signé(s) pourra (ont) lui être envoyé électroniquement en contactant le service client.

## **Article 5 – Convention de preuve**

### **5.1. Valeur probante**

En signant le ou les mandat(s) SEPA proposé(s) sur le site Orange ou Sosh, l'Utilisateur accepte de les télécharger ou de les recevoir par voie électronique. L'utilisateur accepte également de recevoir par voie électronique les modifications ultérieures, et, de manière générale, toute information susceptible de lui être adressée dans le cadre de l'exécution de son contrat.

Il incombe à l'Utilisateur de signaler toute difficulté d'accès à sa messagerie électronique à **Orange**, ceci notamment afin de permettre à **Orange** de lui

faire parvenir les documents nécessaires sur l'adresse mail référencée dans la rubrique « votre compte » de l'espace client Orange.

L'Utilisateur accepte qu'en cas de litige les données transmises, les certificats et signatures électroniques utilisés dans le cadre du Service de contractualisation électroniques soient utilisées devant les tribunaux et fassent preuve des données et des faits qu'ils contiennent ainsi que des signatures et procédés d'authentification qu'ils expriment.

L'Utilisateur accepte qu'en cas de litige, les Jetons d'horodatage soient utilisés devant les tribunaux et fassent preuve des données et des faits qu'elles contiennent.

La preuve des connexions et d'autres éléments d'identification sera établie autant que de besoin à l'appui des journaux de connexion tenus à jour par **Orange**.

L'Utilisateur reconnaît expressément que le fait de cliquer sur le bouton « SIGNER » manifeste son consentement au contenu du contrat et confère à l'écrit signé conformément aux articles 1316-1 et 1316-4 du Code civil la même valeur juridique qu'un document écrit et signé manuscritement.

La signature électronique proposée par le service permet d'assurer l'identification d'**Orange** et de l'Utilisateur signataire, l'authenticité et l'intégrité du contrat souscrit, la manifestation du consentement de l'Utilisateur.

Conformément à la loi, elle donne valeur probante, au même titre que la signature manuscrite :

- aux informations communiquées par **Orange** dans le cadre des offres contractuelles proposées,
- aux informations communiquées par l'Utilisateur.

### **5.2. Archivage**

Il appartient à l'Utilisateur de conserver les documents contractuels pendant toute la durée du contrat qu'il a souscrit..

## **Article 6 – Responsabilité**

### **6.1. Responsabilité de l'Utilisateur**

L'Utilisateur s'engage à prendre toutes les mesures propres à assurer la sécurité et la confidentialité du code d'authentification. Il doit donc, dans son intérêt, le tenir absolument secret et ne pas le communiquer à qui que ce soit et sous quelque forme que ce soit.

L'Utilisateur donne son consentement à l'exécution de son ordre de signature en saisissant, puis validant à l'écran le code d'authentification. Sans préjudice des dispositions applicables au contrat souscrit en ligne, l'engagement contractuel de l'Utilisateur est irrévocable dès qu'il a donné son consentement sous la forme ci-dessus prévue.

## **6.2. Responsabilité d'Orange**

Le contrat et ses accessoires (formulaire, grille tarifaire, etc.) pourront être fournis à la demande de l'Utilisateur.

L'Utilisateur reconnaît que la responsabilité **d'Orange**, ne pourra être engagée dans toutes les hypothèses de modification de sa situation s'il n'a pas transmis par écrit les informations relatives à la modification de sa situation préalablement à la survenance de celle-ci.

La responsabilité **d'Orange**, ne pourra être engagée en cas de force majeure tel que définie par la loi et la jurisprudence des cours et tribunaux français. Il en sera de même dans le cas de l'intrusion d'un tiers sur le poste informatique de l'Utilisateur (virus, logiciels)

### **Article 7 - Données à caractère personnel**

L'Utilisateur sera amené à fournir des données à caractère personnel le concernant en particulier lors de l'adhésion et ce, notamment, pour bénéficier du Service de contractualisation en ligne.

Dans le cadre du bon fonctionnement du Service de contractualisation en ligne, l'Utilisateur donne son consentement explicite à l'utilisation des données à caractère personnel le concernant.

L'Utilisateur dispose d'un droit d'accès, de rectification, de suppression et d'opposition sur les données à caractère personnel le concernant, droits qu'il peut exercer comme suit :

Conformément « Informatique et Libertés » à la loi n°78-17 du 6 janvier 1978 modifiée, l'Utilisateur peut accéder aux données à caractère personnel le concernant. Il peut demander à ce que ses données à caractère personnel inexactes, incomplètes, équivoques ou périmées, soient, selon le cas, rectifiées, complétées, mises à jour ou effacées. Il peut également exercer son droit d'opposition et demander la suppression des données à caractère personnel le concernant. Pour ce faire, il peut effectuer toute demande auprès **d'Orange** par courrier et en joignant un justificatif d'identité, à l'adresse suivante :

Orange Service Clients  
Gestion des données personnelles  
33732 Bordeaux cedex 9

Les données personnelles du client nécessaires à la réalisation des contrats le liant à Orange pourront être transmises à des partenaires commerciaux.

### **Article 8 - Durée**

Les présentes Conditions générales d'utilisation du Service de contractualisation en ligne entrent en vigueur à compter de l'accession au Service de contractualisation en ligne par l'Utilisateur et jusqu'à la fin de la relation avec le client

### **Article 9 - Langue et loi applicable**

En cas de litige relatif à l'interprétation, la formation, la validité ou l'exécution des présentes Conditions générales d'utilisation, l'Utilisateur reconnaît de manière expresse que seule la loi française est applicable.

Seule la langue française lui est proposée pour conclure les contrats objets des présentes Conditions générales d'utilisation du Service de contractualisation en ligne.

### **Article 10 - Modification des conditions d'adhésion en ligne**

**Orange** se réserve le droit d'apporter des modifications aux présentes Conditions générales d'utilisation du Service de contractualisation en ligne.

Toute modification entre en vigueur à compter de sa date de mise en ligne.

### **Article 11 - Intégralité des Conditions générales d'utilisation du Service de contractualisation en ligne**

Les présentes Conditions générales d'utilisation du Service de contractualisation en ligne et leur Annexe « Autorité de Certification User Signing : Conditions Générales d'Utilisation des certificats matériels » acceptées le même jour, expriment seuls l'intégralité des accords entre l'Utilisateur et **Orange** quant à leur objet et remplacent et annulent toutes conventions orales ou écrites, correspondances ou documents antérieurs qu'elles ont pu conclure ou se communiquer ayant un objet identique ou semblable aux présentes Conditions générales d'utilisation du Service de contractualisation en ligne. L'Annexe fait partie intégrante des présentes Conditions générales d'utilisation du service de contractualisation en ligne.

## OBJET DES CGU

Les présentes 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 NA » 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 NA» 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 associée à un Certificat de signature permet la signature des informations et documents du Client présentés au Porteur par le Service de signature électronique.

## 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.

## CONTACT DE L'AUTORITE DE CERTIFICATION

Gouvernance PKI

Autorité de Certification «ALMERYS USER SIGNING CA NA» de l'Infrastructure de Gestion de Clés d'Almerys.

Almerys – 46 rue du Ressort – 63967 CLERMONT-FERRAND CEDEX 9  
Téléphone : 04 73 74 82 98  
gouvernance.igc@almerys.com

## TYPE DE CERTIFICATS EMIS

Les Certificats émis par l'AC « ALMERYS USER SIGNING CA NA » 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 NA »

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

## PRIX

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

## 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.

## 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 1 facteur. Cette identification se base par défaut sur :
  - L'envoi d'un code à usage unique au Porteur par sms ou email.
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 ;
- ➔ 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.

#### **MODALITES DE RENOUELEMENT**

---

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.

#### **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 l'interruption du processus de signature active la fonction de révocation. Cette révocation a pour conséquence la fin de la transaction de signature courante.

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.

#### **LIMITES D'USAGES**

---

Les Certificats émis par l'AC «ALMERYS USER SIGNING CA NA» 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.

#### **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*) et / ou,
- ➔ 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 ;
- ➔ n'utiliser les Certificats délivrés par «ALMERYS USER SIGNING CA NA» qu'à des fins de signature, conformément 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.

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

#### **OBLIGATION DE L'AC**

---

L'AC « ALMERYS USER SIGNING CA NA » 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.

#### **LIMITE DE RESPONSABILITE DE L'AC**

---

Sous réserve des dispositions d'ordre public applicables, l'AC « ALMERYS USER SIGNING CA NA » 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 NA » 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 NA » 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 NA » 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.

#### **DONNEES A CARACTERE PERSONNEL**

---

Toute collecte et tout traitement de données à caractère personnel relatives au Porteur sont réalisés par le Client dans le strict respect de la réglementation en vigueur, et en particulier de la 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, dite « Loi Informatique et Libertés ».

#### **REFERENCES DOCUMENTAIRES**

---

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

<http://pki.almerys.com>

L'OID de cette Politique est 1.2.250.1.16.12.5.41.1.4.1.1.1.

#### **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.

#### **LOI APPLICABLE**

---

Les présentes CGU sont soumises au droit français.

En matière contractuelle, tout litige relatif à la validité, l'interprétation ou l'exécution des présentes CGU sera soumis aux tribunaux compétents de Clermont-Ferrand.

#### **AUDITS ET REFERENCES APPLICABLES**

---

Un contrôle de conformité de l'AC « ALMERYS USER SIGNING CA NA » 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.