



CONDITIONS GÉNÉRALES DU PROCESSUS DE VIDÉO-
IDENTIFICATION ET D'ÉMISSION DE CERTIFICATS DE
LONGUE DURÉE
QES MULTI

*Ceci est une traduction en français de la version anglaise des conditions générales du processus de vidéo-identification et d'émission de certificats de longue durée **QES MULTI**, disponible ici : <https://www.signicat.com/about/english>. Les présentes conditions générales QES MULTI ont été traduites uniquement pour la commodité des SOUSCRIPTEURS ou des DEMANDEURS et n'ont aucune valeur juridique. La version anglaise fait foi en toutes circonstances et prévaut sur la traduction en français.*

D'une part, SIGNICAT, S.L.U (« anciennement dénommée Electronic Identification S.L. »), dont le siège social est situé Avenida Ciudad de Barcelona 81, 4ª Planta, immatriculée au Registre du commerce de Madrid le 13 mars 2013, sous le numéro d'identification B-86681533 (ci-après dénommée « SIGNICAT SLU »), est un Prestataire de services de confiance qualifié, qui agit conformément aux dispositions du règlement (UE) n° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, ainsi qu'aux normes techniques de l'ETSI applicables à l'émission et à la gestion de certificats qualifiés, principalement les normes EN 319 411-1 et EN 319 411-2, afin de faciliter le respect des exigences légales et la reconnaissance internationale de ses services.

Et d'autre part, le DEMANDEUR/SOUSCRIPTEUR, dont les données d'identification aux fins du présent contrat figurent sur sa pièce d'identité utilisée et dans la vidéo générée lors du processus de vidéo-identification et d'émission du certificat.

1. **OBJET**

Le présent document a pour objet d'informer le Demandeur/Souscripteur, de manière claire et compréhensible, des présentes « Conditions générales du processus d'identification à distance par vidéo non assistée et Conditions du service de certification électronique pour l'émission de certificats de longue durée », et de régir les services conformément aux termes prévus dans le présent document, la Déclaration des pratiques de certification, le règlement eIDAS et les lois locales éventuellement applicables.

Ce processus d'identification préalable est nécessaire pour prouver l'identité du Demandeur/Souscripteur, qui demande à SIGNICAT SLU d'émettre un certificat qualifié de signature électronique de personne physique de longue durée (« Services de certification »), certificat dont l'utilisation est soumise aux conditions du service de certification électronique fourni par SIGNICAT SLU en tant que Prestataire de services de confiance qualifié décrites ci-après.

Le certificat électronique qualifié émis en vertu des présentes Conditions générales correspond au profil de certification suivant :

- Certificat qualifié de personne physique dans le CLOUD avec QSCD, OID 1.3.6.1.4.1.55193.1.1.2. Il s'agit d'un certificat qualifié, émis aux fins de signatures électroniques qualifiées et de leur authentification, conformément à la politique de certification QCP-n-qscd, OID 0.4.0.194112.1.2. Ce certificat est émis dans un QSCD centralisé et constitue un certificat qualifié conformément aux dispositions de l'article 28 du règlement (UE) n° 910/2014.

Il fonctionne au moyen de dispositifs de création de signature qualifiés (QSCD), conformément aux articles 29 et 51 du règlement (UE) n° 910/2014, et respecte les dispositions des normes techniques de l'Institut européen des normes de télécommunications, identifiées par la référence ETSI EN 319 411-2. En particulier, le QSCD est le module matériel de sécurité nShield Solo XC v12.60.15 et l'Entrust Signature Activation Module (SAM), version 1.1.1, tous deux

certifiés conformément aux Critères communs EAL4+ et qualifiés en tant que dispositifs de création de signature qualifiés.

Il garantit l'identité du signataire et son lien avec le souscripteur du service électronique de confiance, en permettant la génération de la « *signature électronique qualifiée* », c'est-à-dire la signature avancée, fondée sur un certificat qualifié et générée au moyen d'un dispositif qualifié, équivalant ainsi à la signature manuscrite à toutes fins et effets juridiques, sans qu'il soit nécessaire de remplir d'autres conditions supplémentaires.

2. DÉFINITIONS APPLICABLES

- **AUTORITÉ DE CERTIFICATION (AC)** : entité de confiance de l'émetteur et du destinataire du message. Cette confiance de l'un et de l'autre envers un « tiers de confiance » permet à chacun de se fier à son tour aux documents signés par l'Autorité de certification, en particulier aux documents qui associent chaque clé publique à son titulaire et que l'on appelle certificats. Dans le cadre de la fourniture du Service demandé par le Demandeur/Souscripteur, SIGNICAT SLU agira en tant qu'Autorité de certification en associant une clé publique donnée à un Demandeur/Souscripteur donné par l'émission d'un certificat.
- **AUTORITÉ D'ENREGISTREMENT (AE)** : entité qui, entre autres fonctions, identifie de manière univoque le Demandeur/Souscripteur d'un certificat et, le cas échéant, les autres circonstances liées au Certificat, conformément aux dispositions de la section 1.3.2. « Autorités d'enregistrement » de la DPC de SIGNICAT SLU. L'Autorité d'enregistrement communique à l'Autorité de certification les données vérifiées du Demandeur/Souscripteur afin que l'Autorité de certification émette le certificat correspondant. Tout ou partie des fonctions propres à l'AE peuvent être assumées directement par SIGNICAT SLU ou par toute entité autorisée par SIGNICAT SLU.
- **CERTIFICAT DE SIGNATURE ÉLECTRONIQUE** : attestation électronique qui associe les données de validation d'une signature électronique à une personne physique et confirme au moins le nom ou le pseudonyme de cette personne.
- **CERTIFICAT QUALIFIÉ DE SIGNATURE ÉLECTRONIQUE** : certificat de signature électronique délivré par un Prestataire de services de confiance qualifié et satisfaisant aux exigences fixées à l'annexe I du règlement (UE) n° 910/2014 du 23 juillet 2014 (règlement eIDAS), offrant les garanties juridiques les plus élevées en matière d'identification du signataire et de son lien univoque avec la signature, ainsi que d'intégrité et de non-répudiation des données liées à la signature.
- **DÉCLARATION DES PRATIQUES DE CERTIFICATION (« DPC »)** : document établi par une Autorité de certification qui comprend ou régit la fourniture de Services de certification par ladite Autorité de certification en sa qualité de Prestataire de services de certification, en l'occurrence SIGNICAT SLU. Il régit notamment la gestion des données de création et de vérification de signature et des Certificats, ainsi que les conditions applicables à la demande, à l'émission, à l'utilisation, à la suspension et à la fin de validité des Certificats.

- **SIGNATURE ÉLECTRONIQUE QUALIFIÉE** : signature électronique avancée créée à l'aide d'un dispositif de création de signature électronique qualifié et reposant sur un certificat qualifié de signature électronique. La validité de la signature est présumée (iuris tantum) du fait qu'il s'agit d'une signature qualifiée ; la charge de la preuve incombe à la personne qui conteste la validité de la signature.
- **PRESTATAIRE DE SERVICES DE CONFIANCE QUALIFIÉ** : prestataire de services de confiance qui fournit un ou plusieurs services de confiance qualifiés et a obtenu de l'organe de contrôle le statut qualifié.
- **DEMANDEUR/SOUSCRIPTEUR ou DEMANDEUR/SOUSCRIPTEUR**, c'est-à-dire la personne physique identifiée dans l'en-tête qui souscrit aux services de certification de SIGNICAT SLU et qui, préalablement à l'émission du certificat qualifié, a demandé et mené à bien le processus de vidéo-identification de SIGNICAT SLU.

3. CONDITIONS GÉNÉRALES DU PROCESSUS DE VIDÉO-IDENTIFICATION

Le processus d'identification du Demandeur/Souscripteur pour les services d'identification fournis par SIGNICAT SLU en vue de l'émission de certificats électroniques est réalisé par l'un des moyens suivants, conformément à l'article 24.1 du règlement eIDAS :

- a) en présence de la personne physique ou d'un représentant autorisé de la personne morale, auquel cas le Demandeur/Souscripteur doit se rendre dans les bureaux de SIGNICAT SLU situés Av. de la Ciudad de Barcelona, 81, 4, 28007 Madrid, étant donné qu'il n'existe pas d'Autorités d'enregistrement déléguées ;
- b) à distance, au moyen de moyens d'identification électronique, pour lesquels la présence de la personne physique ou d'un représentant autorisé de la personne morale a été autorisée préalablement à l'émission du certificat qualifié, et conformément au processus de vidéo-identification visé dans le présent document et dans la Déclaration des pratiques de certification, accessible via le lien suivant : <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures> ;
- c) au moyen d'un certificat qualifié de signature électronique ou d'un cachet électronique qualifié délivré conformément au point a) ou b) ;
- d) au moyen d'autres méthodes d'identification reconnues au niveau national qui garantissent une sécurité équivalente à la présence physique en termes de fiabilité. La sécurité équivalente est confirmée par un organisme d'évaluation de la conformité.

3.1 VALIDATION DE L'IDENTITÉ PAR VOIE ÉLECTRONIQUE ET DESCRIPTION DU PROCESSUS DE VIDÉO-IDENTIFICATION

Le processus de vidéo-identification (ci-après le « Processus de vidéo-identification » ou le « Processus ») est une méthode de vérification d'identité à distance par vidéo, en temps réel et non assistée, au

moyen d'une application développée par SIGNICAT SLU et dont elle est propriétaire (l'« Application »), qui met en œuvre, assiste et enregistre l'ensemble du Processus d'enregistrement de la personne et permet de valider des documents d'identité à distance. Cette vidéo capture et valide le document d'identité en temps réel et de manière automatisée (environ 10 à 20 secondes), et est réalisée par SIGNICAT SLU par l'intermédiaire de ses Agents humains qualifiés qui, en tant qu'opérateurs de vérification agissant comme Autorité d'enregistrement, sont chargés d'attester l'identité.

3.1.1 Informations générales sur le Processus de vidéo-identification

Le Demandeur/Souscripteur accède à l'Application et à l'interface avant d'engager les actions permettant de vérifier son identité, **et il lui est demandé de lire le présent document et d'exprimer son acceptation, ainsi que de donner librement son consentement au traitement des données biométriques nécessaires à la réalisation de la vidéo-identification.** À cette fin, SIGNICAT SLU fournit au préalable au Demandeur/Souscripteur la Politique de confidentialité, qui décrit le traitement des données à caractère personnel qui sera effectué pendant le Processus conformément aux dispositions de la réglementation en matière de protection des données.

Si le Demandeur/Souscripteur ne donne pas ce consentement, le Processus ne peut pas se poursuivre et le Demandeur/Souscripteur doit recourir à l'une des autres méthodes d'identification prévues à la clause un du présent document, conformément aux dispositions de l'article 24.1 du règlement eIDAS.

Enfin, avant le début du Processus de vidéo-identification, l'utilisateur sera invité à indiquer un numéro de téléphone afin de recevoir un code OTP permettant d'associer l'identité du Demandeur/Souscripteur à l'appareil et au numéro de téléphone qu'il utilise pour effectuer le Processus.

Une fois que le Demandeur/Souscripteur a lu et accepté le Processus et exprimé son accord, il procède à la vidéo-identification nécessaire afin que SIGNICAT SLU puisse procéder à l'émission du certificat qualifié de personne physique.

Le Demandeur/Souscripteur est guidé à tout moment par la voix et par du texte pendant le Processus de vidéo-identification et, au moyen de l'Application, un contrôle automatisé des éléments de l'environnement (conditions d'éclairage, réseau, qualité de la caméra) est effectué afin d'obtenir un enregistrement optimal de la vidéo-identification et de ses éléments de preuve.

À cet égard, les étapes du Processus préalables à l'émission du certificat qualifié sont les suivantes :

La première étape du Processus indique au Demandeur/Souscripteur qu'il doit présenter le document d'identité à utiliser afin de procéder à une comparaison d'images avec les documents originaux au moyen d'une technologie spécialisée, pour vérifier l'authenticité du document, procéder à l'extraction des données (OCR) de la zone MRZ ou d'autres parties du document, et permettre la consultation des justificatifs en temps réel.

Le recto du document d'identité utilisé par le Demandeur/Souscripteur pendant le Processus est donc capturé. Pour ce faire, il est demandé au Demandeur/Souscripteur de présenter le recto de son document et de cadrer l'image dans le cadre affiché.

Une fois la capture terminée, un message de confirmation s'affiche et le Processus passe à l'étape

suivante.

L'étape suivante consiste à capturer le verso du document. Il est demandé au Demandeur/Souscripteur de présenter le verso de son document et de cadrer l'image dans le cadre affiché.

Une fois la capture terminée, un message de confirmation s'affiche et le Processus passe à l'étape suivante.

Les données biométriques du Demandeur/Souscripteur sont ensuite capturées afin d'effectuer une comparaison en temps réel avec l'image du document d'identité, dans le cadre d'un processus de reconnaissance faciale fondé sur une notation biométrique automatique. À cette fin, il est demandé au Demandeur/Souscripteur de montrer son visage et de cadrer l'image dans le cadre affiché à l'écran.

Une fois les données biométriques capturées, il est demandé au Demandeur/Souscripteur, à titre de preuve de vie, d'effectuer un mouvement du visage devant la caméra et, si tout est correct, un message de conformité s'affiche et le Processus passe à l'étape suivante.

Lorsque l'ensemble du Processus s'est déroulé avec succès, le Demandeur/Souscripteur est informé que le Processus de vidéo-identification est terminé et que les éléments de preuve générés pendant le Processus seront contrôlés et validés au moyen de l'Outil de vérification de l'Autorité d'enregistrement, pour examen du Processus par une personne qualifiée ayant suivi au préalable une formation spécifique.

À ce stade, l'Application met la vidéo-identification et les données générées au cours de celle-ci à la disposition d'un Agent humain qualifié chargé de vérifier l'identité du Demandeur/Souscripteur du Processus, et demande l'examen asynchrone de la vidéo enregistrée ainsi que des autres éléments de preuve et éléments obtenus pendant le Processus. Le temps moyen de vérification par un agent est d'environ trois minutes.

3.1.2. Éléments de sécurité du Processus de vidéo-identification et validation par un Agent humain qualifié

Pour l'examen asynchrone par un Agent humain qualifié, il existe un protocole de sécurité fondé sur les bonnes pratiques de l'UE, appuyé par l'outil mis à la disposition de l'Agent humain qualifié, dans lequel sont présentés les éléments de preuve obtenus pendant le Processus, ainsi que les alertes ou notifications concernant ceux qui n'ont pas été obtenus.

L'enregistrement de la vidéo, la demande de vérification de la vidéo-identification ainsi que la décision de l'Agent qualifié sont tracés dans l'Application, et un horodatage est appliqué à chaque trace afin d'en garantir la cohérence et l'intégrité.

Le Processus garantit ainsi la chaîne de traçabilité de la vérification, depuis les éléments de preuve recueillis par le Processus jusqu'aux traces reliant l'identification à l'Agent humain qualifié de l'Autorité d'enregistrement. Il en résulte une identité vérifiée offrant une sécurité technique équivalente à celle d'une vérification effectuée en présence physique du Demandeur/Souscripteur.

Une fois l'identité validée favorablement par l'Agent humain qualifié, l'identité du Demandeur/Souscripteur est attestée et celui-ci peut poursuivre et bénéficier du Service de certification électronique de SIGNICAT SLU, qui lui permet de poursuivre le processus d'émission du certificat qualifié de personne physique et la signature de documents électroniques.

Si le résultat du Processus est négatif, le Processus d'émission de certificats qualifiés ne peut pas se poursuivre et le Demandeur/Souscripteur doit se rendre physiquement dans les locaux de SIGNICAT SLU afin de faire vérifier son identité en personne.

3.2 OBLIGATIONS DU DEMANDEUR/SOUSCRIPTEUR EN RELATION AVEC LE PROCESSUS DE VIDÉO-IDENTIFICATION.

Le Demandeur/Souscripteur, tout au long du Processus, s'engage à :

- Utiliser le Service conformément aux dispositions du présent document, de la DPC, des conditions particulières éventuellement applicables et de toute autre instruction, tout manuel ou toute procédure fourni par SIGNICAT SLU.
- Veiller à ce que le document utilisé pendant le Processus soit un document authentique et juridiquement valable et, en outre :
 - qu'il ne s'agisse pas d'une photocopie ni d'une carte imprimée ;
 - qu'il ne soit pas au format numérique (téléphone mobile, tablette ou ordinateur) ;
 - qu'il ne soit pas placé dans un étui ;
 - qu'il ne soit pas endommagé et soit complet, tous les éléments de sécurité figurant sur le document.
- Veiller à ce que, pendant le Processus et l'enregistrement de la vidéo, afin d'éviter un rejet :
 - les conditions d'éclairage de la vidéo permettent de voir clairement le visage de la personne identifiée et le document ;
 - le flux vidéo soit continu, sans coupures ni retards ;
 - ce soit une personne vivante qui présente la pièce d'identité ;
 - si une personne autre que la personne à identifier réalise l'ensemble du Processus, l'identification sera rejetée comme non authentique ;
 - si une autre personne est présente dans la vidéo mais n'exerce manifestement aucune contrainte sur la personne à identifier, l'identification peut être valable, par exemple lorsqu'une personne aide une personne handicapée à réaliser l'identification ;
 - il soit possible de visualiser clairement toutes les parties des captures du document, recto, verso et visage de la personne ;
 - le Demandeur/Souscripteur ne soit pas endormi et ne présente aucun signe pouvant être interprété comme étant sous l'influence de drogues ou d'alcool.

3.3 ÉMISSION, REMISE ET ACCEPTATION DU CERTIFICAT

3.3.1 Demande de certificat et génération des clés par SIGNICAT SLU pour le compte du

Demandeur/Souscripteur.

Une fois le Processus de vidéo-identification terminé, le Demandeur/Souscripteur demande et autorise SIGNICAT SLU à générer et gérer, le cas échéant, en son nom les clés privée et publique, ce qui permet à SIGNICAT SLU de procéder à l'émission du certificat qualifié de longue durée de personne physique et de signer en son nom les documents électroniques appropriés avec des tiers de nature publique ou privée avec lesquels SIGNICAT SLU entretient certains accords contractuels, conformément aux dispositions des clauses 3.3.3, 3.3.4 et 3.3.5.

3.3.2 Véracité des informations

Le DEMANDEUR/SOUSCRIPTEUR est tenu de veiller à ce que toutes les informations fournies à SIGNICAT SLU, directement ou au moyen du document d'identité utilisé lors du processus d'émission du certificat, soient exactes, complètes au regard de l'objet du certificat et à jour à tout moment ; à cette fin, il garantit utiliser un document d'identité légal et valable, qui n'a pas été altéré ni modifié par le DEMANDEUR/SOUSCRIPTEUR ou par des tiers.

3.3.3 Émission du certificat

Pour l'émission du certificat, SIGNICAT SLU utilise les données du document d'identité fourni par le Demandeur/Souscripteur pendant le Processus de vidéo-identification. Ces données sont extraites par SIGNICAT SLU et intégrées au certificat électronique afin d'y associer son identité, après confirmation par le Demandeur/Souscripteur.

3.3.4 Réception du code PIN

Une fois le processus de vidéo-identification terminé, nous vous enverrons un code PIN qui sera associé à votre certificat électronique.

Ce code PIN sera utilisé pour signer des documents comme prévu à la clause 3.4.

Le code PIN est un code secret que seul le Demandeur/Souscripteur doit connaître, car le contrôle exclusif de ce code PIN garantit le contrôle exclusif du certificat électronique pour la signature des documents ; par conséquent, ce code PIN ne doit être connu que de l'utilisateur, qui ne doit pas le divulguer à des tiers, car il est personnel et inaccessible.

Si l'utilisateur perd le code PIN ou soupçonne que des tiers peuvent le connaître, il doit en informer immédiatement SIGNICAT SLU afin de révoquer le certificat électronique.

L'utilisation de ce code PIN pour signer des documents vaut expression du consentement du Demandeur/Souscripteur à être lié par leur contenu.

3.3.5 Acceptation de l'émission du certificat et ratification des présentes Conditions générales.

Une fois le code PIN reçu, le Demandeur/Souscripteur doit confirmer qu'il est en sa possession.

Pour ce faire, il doit le saisir afin d'accepter l'émission du certificat électronique ainsi que les présentes Conditions générales, qui vous seront présentées au préalable et vous seront ensuite envoyées par

courrier électronique, déjà signées électroniquement par le Demandeur/Souscripteur.

3.3.6 Remise du certificat

Dans le cadre du processus d'émission, il n'y a pas de remise spécifique du certificat au Demandeur/Souscripteur. SIGNICAT SLU le gère en sa qualité de Prestataire de services de confiance qualifié, afin que le Demandeur/Souscripteur puisse l'utiliser pour la signature électronique de documents.

3.4 SERVICE DE SIGNATURE SUR SERVEUR

Une fois le processus d'identification terminé et l'identité validée par l'agent de vérification, l'identité du Signataire est garantie et SIGNICAT SLU, en tant que Prestataire de services de confiance qualifié, conserve en toute sécurité le certificat électronique de l'utilisateur afin que celui-ci puisse l'utiliser pendant sa durée de validité pour signer des documents électroniquement.

Chaque fois que l'utilisateur souhaite signer électroniquement un document à l'aide du certificat électronique généré, il doit accéder à l'espace dédié où il peut en consulter le contenu.

S'il est satisfait du contenu et souhaite s'engager au moyen de sa signature électronique, l'utilisateur doit poursuivre le processus.

La plateforme lui demande alors son code PIN, qui garantit le contrôle exclusif de l'utilisateur sur son certificat électronique.

Une fois le code PIN saisi, il reçoit sur son téléphone mobile un code OTP qu'il doit saisir dans la section prévue à cet effet dans l'environnement de signature. La saisie de ce code OTP permet à SIGNICAT SLU d'appliquer les données de création de signature du Demandeur/Souscripteur afin de générer la signature électronique du document préalablement affiché.

SIGNICAT SLU concède au Demandeur/Souscripteur, à titre non exclusif et incessible, une licence d'utilisation des copies du logiciel du dispositif cryptographique sécurisé de SIGNICAT SLU pour le fonctionnement du dispositif de signature, le cas échéant, ainsi que pour la production de la signature électronique, du certificat et des autres services cryptographiques par les signataires.

Si une personne autre que SIGNICAT SLU apporte des modifications au logiciel fourni, toutes les garanties relatives au logiciel seront immédiatement annulées.

4. CONDITIONS GÉNÉRALES DU SERVICE DE CONFIANCE

4.1 CONDITIONS GÉNÉRALES DU SERVICE DE VIDÉO-IDENTIFICATION

- Durée de conservation des informations

Toutes les informations relatives au Processus d'émission de certificats électroniques qualifiés de personnes physiques, y compris les informations biométriques, sont conservées par SIGNICAT SLU

pendant la durée de la relation contractuelle, tant que leur suppression n'est pas demandée, et pendant le délai de prescription des actions en justice susceptibles d'être intentées ou des réclamations susceptibles d'être reçues de la part d'organismes officiels.

À cet égard, la durée maximale de conservation des informations pertinentes relatives au Processus de vidéo-identification et d'émission de certificats qualifiés, à savoir une copie de l'enregistrement vidéo, les photos ou captures d'écran du Demandeur/Souscripteur et du document d'identité utilisé, le résultat automatique de la vérification effectuée par l'Application de SIGNICAT SLU, ainsi que l'évaluation et les observations des Agents humains qualifiés de vérification d'identité, accompagnées de leur décision d'approuver ou de rejeter l'identification, est de 15 ans à compter de la révocation ou de l'expiration du certificat, sauf disposition légale contraire. Une fois la relation contractuelle terminée, les données du Demandeur/Souscripteur seront dûment bloquées, conformément aux dispositions de la réglementation applicable.

En outre, il est précisé que tous les éléments de preuve des processus d'identification inachevés, interrompus en raison d'une suspicion de tentative de fraude, seront conservés pendant une durée de 5 ans à compter de l'exécution du Processus, avec indication du motif de leur interruption, conformément à la politique établie à cet effet.

- **Limitation de responsabilité en relation avec le Processus de vidéo-identification.**

Qualité du Processus : SIGNICAT SLU garantit le bon fonctionnement des Services de vidéo-identification décrits dans le présent document, à condition que les moyens mis à la disposition du Demandeur/Souscripteur soient utilisés correctement et conformément aux instructions de SIGNICAT SLU.

L'accès aux Services de vidéo-identification et leur utilisation n'impliquent pas d'obligation pour SIGNICAT SLU de contrôler l'absence de virus, de vers ou de tout autre élément informatique nuisible. Il appartient au Demandeur/Souscripteur, en tant qu'utilisateur, de disposer à tout moment d'outils adéquats de détection et de désinfection des programmes informatiques nuisibles. SIGNICAT SLU ne saurait être tenue responsable des dommages causés à l'équipement informatique du Demandeur/Souscripteur ou de tiers pendant le Processus de vidéo-identification.

Disponibilité du Processus : le fonctionnement du Processus de vidéo-identification peut dépendre de la configuration correcte de l'équipement à partir duquel l'utilisateur accède au Processus de vidéo-identification et le lance ; l'utilisateur doit donc suivre les instructions fournies et, en tout état de cause, satisfaire à tout moment aux exigences logicielles et matérielles spécifiées.

De même, une ligne d'accès à Internet doit être disponible pour réaliser le Processus de vidéo-identification. Le fonctionnement du Processus de vidéo-identification peut dépendre de la qualité et du débit adéquats de la connexion par laquelle le Demandeur/Souscripteur accède à l'application, le Demandeur/Souscripteur étant seul responsable de la fourniture des lignes de télécommunication, des abonnements ou connexions à Internet ou de tout autre moyen technique nécessaire pour accéder à ses données et les utiliser.

SIGNICAT SLU ne saurait être tenue responsable des dommages découlant de l'inexécution ou de la mauvaise exécution des obligations du Demandeur/Souscripteur ou liés à celles-ci, ni de l'utilisation incorrecte des résultats du Processus et des clés, ni de tout dommage indirect pouvant résulter de l'utilisation du Processus ou des informations fournies par SIGNICAT SLU.

SIGNICAT SLU ne saurait être tenue responsable des inexactitudes dans l'identification du Demandeur/Souscripteur résultant des informations fournies par ce dernier pendant le Processus.

SIGNICAT SLU ne saurait être tenue responsable du bon fonctionnement d'applications non homologuées, ni des dommages résultant de l'impossibilité pour le Demandeur/Souscripteur d'utiliser lesdites applications.

4.2 CONDITIONS GÉNÉRALES DES SERVICES DE CERTIFICATION ÉLECTRONIQUE DE CERTIFICATS DE LONGUE DURÉE.

- Cadre juridique de la fourniture du Service

Les services de certification de SIGNICAT SLU sont régis, sur le plan technique et opérationnel, par la Déclaration des pratiques de certification et les Politiques de certification de SIGNICAT SLU et leurs mises à jour ultérieures, ainsi que par la documentation complémentaire fournie au DEMANDEUR/SOUSCRIPTEUR.

Les présentes conditions générales, la Déclaration des pratiques de certification et les Politiques de certification, lorsqu'elles s'appliquent au certificat émis, constituent le cadre juridique qui régit la relation entre SIGNICAT SLU et le DEMANDEUR/SOUSCRIPTEUR, tant entre les parties qu'à l'égard des tiers, sans préjudice des dispositions de la législation en vigueur.

Le présent document expose les aspects et exigences les plus importants des droits et obligations des parties.

La Déclaration des pratiques de certification (DPC) et les Politiques de certification spécifiques (PC) applicables sont intégrées par référence au présent document. La dernière version à jour de la DPC est accessible à tout moment et gratuitement dans les langues suivantes, via le lien ci-dessous :

Espagnol : <https://www.signicat.com/es/acerca-de/certificados-cualificados-para-firma-electronica>

Anglais : <https://www.signicat.com/about/qualified-certificates-for-electronic-signatures>

En cas de divergence, le sens des termes figurant dans le présent document prévaut sur ce qui est énoncé dans la DPC.

- Durée du contrat

Le présent Contrat est valable pendant la période comprise entre les dates d'émission et d'expiration indiquées dans le Certificat qualifié de personne physique demandé et souscrit par le Demandeur/Souscripteur auprès de SIGNICAT SLU.

- Obligations d'utilisation correcte

Le DEMANDEUR/SOUSCRIPTEUR doit utiliser le service de certification fourni par SIGNICAT SLU exclusivement pour les usages autorisés dans la DPC, que le DEMANDEUR/SOUSCRIPTEUR connaît et accepte pour avoir lu le document et coché les cases de sélection prévues dans le processus.

Le DEMANDEUR/SOUSCRIPTEUR s'engage à utiliser le service de certification numérique et tout autre élément technique remis par SIGNICAT SLU, ainsi que les certificats, conformément aux présentes conditions générales, à la DPC et aux PC éventuellement applicables, aux conditions particulières énoncées dans le manuel le cas échéant, ainsi qu'à toute autre instruction ou procédure fournie par SIGNICAT SLU au DEMANDEUR/SOUSCRIPTEUR, et dans le respect de toute disposition légale en vigueur.

La souscription du Service de certification auprès de SIGNICAT SLU n'autorise l'utilisation du Certificat que dans le cadre de l'activité officielle du DEMANDEUR/SOUSCRIPTEUR, conformément à la finalité du type de certificat demandé, à savoir le certificat qualifié de signature électronique de personne physique de longue durée. Une fois le certificat émis, le DEMANDEUR/SOUSCRIPTEUR ne peut, sauf accord spécifique contraire entre les parties, utiliser le certificat à des fins commerciales. Par utilisation commerciale du certificat, on entend toute action par laquelle le DEMANDEUR/SOUSCRIPTEUR offre à des tiers, en dehors du présent contrat, à titre onéreux ou gratuit, des services nécessitant l'utilisation du certificat émis.

- **Opérations interdites**

Les services de certification numérique fournis par SIGNICAT SLU n'ont pas été conçus ni autorisés pour être utilisés ou revendus comme équipements de contrôle de situations dangereuses, ou pour des usages exigeant des actions infaillibles, tels que l'exploitation d'installations nucléaires, de systèmes de navigation ou de communication aérienne, de systèmes de contrôle du trafic aérien ou de systèmes de contrôle d'armements, où une erreur pourrait directement entraîner la mort, des dommages corporels ou de graves dommages environnementaux.

- **Obligations et responsabilités de SIGNICAT SLU**

a) En ce qui concerne la fourniture du Service en tant qu'Autorité d'enregistrement.

SIGNICAT SLU s'engage à enregistrer les données du certificat et à émettre ensuite celui-ci au profit du DEMANDEUR/SOUSCRIPTEUR, et doit à cette fin effectuer les vérifications qu'elle juge nécessaires concernant l'identité et les autres informations personnelles et complémentaires du DEMANDEUR/SOUSCRIPTEUR et, le cas échéant, des Signataires eux-mêmes.

Ces vérifications doivent porter sur les justificatifs fournis par le DEMANDEUR/SOUSCRIPTEUR et, si SIGNICAT SLU le juge nécessaire, sur tout autre document et toute autre information pertinents fournis par le DEMANDEUR/SOUSCRIPTEUR.

Si SIGNICAT SLU détecte des erreurs dans les données qui doivent figurer dans les certificats ou dans les éléments qui les justifient, elle peut apporter les modifications qu'elle juge nécessaires avant d'émettre le certificat, ou suspendre le processus d'émission et traiter l'incident correspondant avec le DEMANDEUR/SOUSCRIPTEUR.

Si SIGNICAT SLU corrige les données sans avoir traité au préalable l'incident correspondant avec le

DEMANDEUR/SOUSCRIPTEUR, elle doit notifier au DEMANDEUR/SOUSCRIPTEUR les données finalement certifiées.

SIGNICAT SLU se réserve le droit de ne pas émettre le certificat lorsque les justificatifs fournis sont insuffisants pour l'identification et l'authentification correctes du DEMANDEUR/SOUSCRIPTEUR, ou lorsque le Processus de vidéo-identification réalisé préalablement à l'émission du certificat n'a pas été confirmé comme valable par SIGNICAT SLU.

Les obligations ci-dessus seront suspendues si le DEMANDEUR/SOUSCRIPTEUR agit en tant qu'Autorité d'enregistrement et dispose des éléments techniques correspondant à la génération de clés et à l'émission de certificats.

b) En ce qui concerne la fourniture du Service de certification.

SIGNICAT SLU s'engage à respecter les obligations établies par la loi 6/2020 du 11 novembre, qui réglemente certains aspects des services électroniques de confiance, et notamment à :

- a) Émettre, remettre, gérer, suspendre, révoquer et renouveler les certificats, conformément aux instructions fournies par le DEMANDEUR/SOUSCRIPTEUR, dans les cas et pour les motifs décrits dans la DPC de SIGNICAT SLU.
- b) Exécuter les services avec les moyens techniques et matériels appropriés, et avec un personnel répondant aux conditions de qualification et d'expérience pertinente fixées dans la DPC.
- c) Respecter les niveaux de qualité de service, conformément à ce qui est établi dans la DPC, sur les plans technique, opérationnel et de la sécurité.
- d) Communiquer l'état des certificats, conformément à ce qui est établi dans la DPC pour les différents services de vérification des certificats, aux tiers qui en font la demande.
- e) Qualité du Processus : SIGNICAT SLU garantit le bon fonctionnement des Services de certification décrits dans le présent document, à condition que les moyens mis à la disposition du DEMANDEUR/SOUSCRIPTEUR soient utilisés correctement et conformément aux instructions de SIGNICAT SLU.

L'accès aux Services de certification et leur utilisation n'impliquent pas d'obligation pour SIGNICAT SLU de contrôler l'absence de virus, de vers ou de tout autre élément informatique nuisible. Il appartient au DEMANDEUR/SOUSCRIPTEUR, en tant qu'utilisateur, de disposer à tout moment d'outils adéquats de détection et de désinfection des programmes informatiques nuisibles. SIGNICAT SLU ne saurait être tenue responsable des dommages causés à l'équipement informatique du DEMANDEUR/SOUSCRIPTEUR ou de tiers pendant le Processus de vidéo-identification.

- f) Disponibilité du Processus : le fonctionnement du Processus de certification peut dépendre de la configuration correcte de l'équipement à partir duquel l'utilisateur accède au processus de vidéo-identification et le lance ; l'utilisateur doit donc suivre les instructions fournies et, en tout état de cause, satisfaire à tout moment aux exigences logicielles et matérielles spécifiées.

De même, une ligne d'accès à Internet doit être disponible pour réaliser le Processus de vidéo-identification. Le fonctionnement du Processus de vidéo-identification peut dépendre de la qualité et du débit adéquats de la connexion par laquelle le DEMANDEUR/SOUSCRIPTEUR accède à l'application, le DEMANDEUR/SOUSCRIPTEUR étant seul responsable de la fourniture des lignes de télécommunication, des abonnements ou connexions à Internet ou de tout autre moyen technique nécessaire pour accéder à ses données et les utiliser.

- **En tant que Prestataire de services de certification.**

SIGNICAT SLU doit :

- a) Publier des informations véridiques conformément à la loi 6/2020 du 11 novembre, qui réglemente certains aspects des services électroniques de confiance, et au règlement (UE) n° 910/2014.
- b) Ne pas stocker ni copier, elle-même ou par l'intermédiaire d'un tiers, les données de création de signature, sauf dans le cas de leur gestion pour le compte du titulaire aux fins de l'application des clés privées pour la création de signature, selon les instructions données par le DEMANDEUR/SOUSCRIPTEUR au moyen du système OTP que SIGNICAT SLU met à la disposition du DEMANDEUR/SOUSCRIPTEUR pour la signature de documents électroniques. Dans ce cas, elle utilise des systèmes et produits fiables, y compris des canaux de communication électronique sécurisés, et applique des procédures et mécanismes techniques et organisationnels appropriés afin de garantir que l'environnement est fiable et utilisé sous le contrôle exclusif du titulaire du certificat. En outre, elle doit préserver et protéger les données de création de signature contre toute altération, destruction ou tout accès non autorisé, et en garantir la disponibilité continue.
- c) Proposer un service de consultation, accessible au public, de l'état de validité ou de révocation des certificats émis.
- d) Respecter les obligations supplémentaires suivantes :
 - 1. La durée pendant laquelle les informations relatives aux services fournis doivent être conservées, conformément à l'article 24.2.h) du règlement (UE) n° 910/2014, est de 15 ans à compter de l'expiration du certificat ou de la fin du service fourni. Lorsque des certificats qualifiés de cachet électronique ou d'authentification de site Internet sont délivrés à des personnes morales, les prestataires de services de confiance enregistrent également les informations permettant de déterminer l'identité de la personne physique à laquelle lesdits certificats ont été remis, aux fins de son identification dans le cadre de procédures judiciaires ou administratives.
 - 2. Souscrire une assurance de responsabilité civile d'un montant minimum de 1 500 000 euros, sauf si le prestataire appartient au secteur public. Si plus d'un des services qualifiés prévus par le règlement (UE) n° 910/2014 est fourni, un montant supplémentaire de 500 000 euros s'ajoute pour chaque type de service supplémentaire. Ladite garantie peut être remplacée en tout ou partie par une garantie bancaire ou une assurance caution, de sorte que la somme des montants assurés soit conforme aux dispositions du paragraphe précédent. Les montants ainsi que les moyens d'assurance et de garantie établis aux deux paragraphes précédents peuvent être modifiés par décret royal.

3. En cas de cessation de son activité en tant que Prestataire de services de confiance qualifié, informer les clients auxquels elle fournit les services ainsi que l'organe de contrôle au moins deux mois avant la cessation effective de l'activité, par un moyen attestant la remise et la réception effectives lorsque cela est possible. Le plan de cessation d'activité du prestataire peut prévoir le transfert des clients, après constatation de l'absence d'opposition, à un autre prestataire qualifié, qui pourra conserver toute information relative aux services fournis jusqu'alors. De même, elle informe l'organe de contrôle de toute autre circonstance pertinente susceptible d'empêcher la poursuite de ses activités. En particulier, elle doit signaler l'ouverture de toute procédure d'insolvabilité engagée à son encontre dès qu'elle en a connaissance.

4. Transmettre le rapport d'évaluation de la conformité au ministère des Affaires économiques et de la Transformation numérique dans les conditions prévues à l'article 20.1 du règlement (UE) n° 910/2014. Le non-respect de cette obligation entraînera le retrait du statut qualifié du prestataire et du service qu'il fournit, ainsi que sa radiation de la liste de confiance prévue à l'article 22 dudit règlement, après mise en demeure du prestataire de services de mettre fin audit manquement.

e) SIGNICAT SLU assume l'entière responsabilité à l'égard des tiers des actes des personnes ou autres prestataires de services auxquels elle délègue l'exécution de tout ou partie des fonctions nécessaires à la fourniture de services électroniques de confiance, y compris les actes de vérification d'identité préalables à l'émission d'un certificat qualifié.

- **GARANTIES RELATIVES AUX SERVICES DE CERTIFICATION**

Garantie de SIGNICAT SLU relative aux services de certification électronique.

SIGNICAT SLU garantit que la clé privée de l'Autorité de certification utilisée pour émettre les certificats n'a pas été compromise, sauf communication contraire par le biais du registre de certification, conformément à la DPC.

SIGNICAT SLU garantit uniquement au DEMANDEUR/SOUSCRIPTEUR, au moment de l'émission du certificat, que :

- a) le cas échéant, les certificats sont qualifiés au sens de la loi 6/2020 du 11 novembre, qui régit certains aspects des services électroniques de confiance ;
- b) SIGNICAT SLU n'a ni produit ni introduit de déclarations fausses ou erronées dans les informations contenues dans un certificat, ni omis d'y inclure des informations nécessaires fournies et vérifiées par le DEMANDEUR/SOUSCRIPTEUR ;
- c) tous les certificats satisfont aux exigences de forme et de contenu énoncées dans la DPC et les PC de SIGNICAT SLU ;
- d) SIGNICAT SLU a respecté les procédures décrites dans la DPC.

SIGNICAT SLU fait preuve d'une diligence raisonnable pour garantir que chaque produit fourni dans le cadre de ses services est exempt de virus informatiques, de vers et d'autres codes illicites, et s'engage à informer le DEMANDEUR/SOUSCRIPTEUR de tout virus, ver ou autre code illicite découvert ultérieurement dans un produit.

- **EXCLUSIONS DE GARANTIE**

SIGNICAT SLU ne garantit aucun logiciel utilisé par le DEMANDEUR/SOUSCRIPTEUR du certificat ou par le Signataire, ou par toute autre personne, pour générer, vérifier ou utiliser de toute autre manière une signature numérique ou un certificat numérique émis par SIGNICAT SLU, sauf déclaration écrite contraire de SIGNICAT SLU.

- **LIMITATIONS DE RESPONSABILITÉ EN TANT QUE PRESTATAIRE DE SERVICES ÉLECTRONIQUES DE CONFIANCE.**

SIGNICAT SLU, dans les limites établies par la loi applicable, ne saurait être tenue responsable des dommages et pertes causés à la personne à laquelle elle a fourni ses services ou aux tiers de bonne foi, lorsque ceux-ci surviennent dans l'un des cas prévus par le règlement (UE) n° 910/2014 ou dans les cas suivants :

- a) Défaut de communication au prestataire de services de confiance d'informations véridiques, complètes et exactes pour la fourniture du service de confiance, en particulier sur les données devant figurer dans le certificat électronique ou nécessaires à son émission, à son extinction ou à la suspension de sa validité, dès lors que leur inexactitude n'a pas été détectée par le prestataire de services agissant avec la diligence requise.
- b) Défaut de communication sans retard injustifié à SIGNICAT SLU de toute modification des circonstances ayant une incidence sur la fourniture du service de confiance, en particulier celles qui figurent dans le certificat électronique.
- c) Négligence dans la conservation des données de création de signature ou d'authentification de site Internet, dans la garantie de leur confidentialité et dans la protection contre tout accès à celles-ci ou toute divulgation de celles-ci ou, le cas échéant, des moyens qui y donnent accès.
- d) Le fait de ne pas demander la suspension ou la révocation du certificat électronique en cas de doute quant au maintien de la confidentialité des données de création de signature, de cachet ou d'authentification de site Internet ou, le cas échéant, des moyens qui y donnent accès.
- e) Le fait d'utiliser les données de création de signature, de cachet ou d'authentification de site Internet après l'expiration de la période de validité du certificat électronique, ou lorsque le prestataire de services de confiance vous notifie l'extinction ou la suspension de sa validité.

SIGNICAT SLU ne saurait non plus être tenue responsable des dommages si le destinataire agit avec négligence.

Le destinataire est réputé agir avec négligence lorsqu'il ne tient pas compte de la suspension ou de la perte de validité du certificat électronique, ou lorsqu'il ne vérifie pas la signature ou le cachet électronique.

SIGNICAT SLU ne saurait être tenue responsable des dommages en cas d'inexactitude des données contenues dans le certificat électronique si celles-ci ont été attestées au moyen d'un document public ou officiel, ou inscrites dans un registre public lorsque cela est requis.

- **RESPONSABILITÉ DU DEMANDEUR/SOUSCRIPTEUR**

Le DEMANDEUR/SOUSCRIPTEUR répond envers toute personne du manquement à ses obligations, notamment en ce qui concerne l'activité d'identification ou, le cas échéant, d'Autorité d'enregistrement, conformément aux présentes Conditions générales.

Le DEMANDEUR/SOUSCRIPTEUR est responsable de toutes les communications électroniques authentifiées au moyen d'une signature numérique générée avec sa clé privée, dès lors que le certificat a été valablement vérifié selon les mécanismes et conditions définis par SIGNICAT SLU.

Tant que la notification prévue dans le présent document n'a pas eu lieu, toute responsabilité pouvant découler de l'utilisation non autorisée et/ou abusive des certificats incombe au DEMANDEUR/SOUSCRIPTEUR.

- **ADÉQUATION DES PRODUITS UTILISANT L'IDENTIFICATION, LA SIGNATURE ÉLECTRONIQUE OU LE CHIFFREMENT**

SIGNICAT SLU ne saurait être tenue responsable de l'adéquation des produits et services de certification numérique, d'identification, de signature électronique ou de chiffrement existant sur le marché et utilisés dans les applications informatiques du DEMANDEUR/SOUSCRIPTEUR, sauf lorsque SIGNICAT SLU les fournit. Dans ce cas, les parties seront soumises aux conditions d'utilisation correspondantes.

- **PROPRIÉTÉ DES CERTIFICATS**

Les certificats fournis demeurent la propriété du DEMANDEUR/SOUSCRIPTEUR.

- **RÉSILIATION**

La résiliation intervient dans les cas suivants :

- a) En cas de manquement de l'autre partie à l'une de ses obligations, s'il n'a pas été remédié à ce manquement :
- b) dans un délai de trente jours à compter de la réception de la notification adressée par la partie qui n'a pas manqué à ses obligations ;
- c) immédiatement, si le manquement compromet la sécurité des services.
- d) En cas de survenance de toute autre cause de résiliation anticipée prévue par la législation en vigueur et, en particulier, par la législation en vigueur en matière de signature électronique et de certification numérique.

- **POLITIQUE DE CONFIDENTIALITÉ**

SIGNICAT SLU ne peut divulguer, ni être contrainte de divulguer, aucune information confidentielle

relative aux certificats sans une demande préalable spécifique émanant :

- a) de la personne à l'égard de laquelle SIGNICAT SLU est tenue de préserver la confidentialité des informations, ou
- b) d'une ordonnance judiciaire, administrative ou de toute autre décision prévue par la législation en vigueur.

Toutefois, le DEMANDEUR/SOUSCRIPTEUR accepte que certaines informations, personnelles ou non, fournies dans la demande de certificat soient incluses dans ses certificats et dans le mécanisme de vérification de l'état des certificats, et que lesdites informations ne soient pas considérées comme confidentielles en vertu d'une obligation légale.

- **POLITIQUE DE REMBOURSEMENT**

SIGNICAT SLU ne rembourse en aucun cas le coût du service de certification.

- **DURÉE DE CONSERVATION DES INFORMATIONS**

Toutes les informations relatives au Processus d'émission de certificats électroniques qualifiés de personnes physiques, y compris le contrat dûment formalisé par le DEMANDEUR/SOUSCRIPTEUR et les journaux générés tout au long de l'émission, sont conservées par SIGNICAT SLU pendant la durée de la relation contractuelle, tant que leur suppression n'est pas demandée, et pendant le délai de prescription des actions en justice susceptibles d'être intentées ou des réclamations susceptibles d'être reçues de la part d'organismes officiels.

À cet égard, la durée maximale de conservation des informations pertinentes relatives au Processus d'émission de certificats qualifiés est de 15 ans à compter de la révocation ou de l'expiration du certificat, sauf disposition légale contraire. Une fois la relation contractuelle terminée, les données du DEMANDEUR/SOUSCRIPTEUR seront dûment bloquées, conformément aux dispositions de la réglementation applicable.

5. DISPOSITIONS COMMUNES

5.1. LIEU D'EXERCICE DE L'ACTIVITÉ

Le lieu d'exécution des obligations de SIGNICAT SLU relatives aux services de certification numérique et, le cas échéant, aux licences d'utilisation de logiciels, est le siège social de SIGNICAT SLU.

5.2. DIVISIBILITÉ DES CONDITIONS GÉNÉRALES

Les clauses du présent document sont indépendantes les unes des autres ; par conséquent, si une clause est jugée nulle ou inapplicable, les autres clauses continueront de s'appliquer, sauf accord exprès contraire des parties.

5.3. RÉGLEMENTATION APPLICABLE ET JURIDICTION COMPÉTENTE.

Les relations avec SIGNICAT SLU sont régies par les dispositions du règlement (UE) n° 910/2014 (eIDAS),

par le droit espagnol et, en particulier, par toutes celles qui découlent de sa politique de conformité.

La juridiction compétente est celle indiquée dans la loi 1/2000 du 7 janvier relative à la procédure civile, sauf lorsque le DEMANDEUR/SOUSCRIPTEUR est considéré comme un consommateur, auquel cas SIGNICAT SLU se soumettra à la juridiction légalement compétente.