

1. OBJET

Les présentes conditions ont pour objet de préciser les conditions générales d'utilisation (CGU) des CERTIFICATS délivrés par l'autorité « TESSI CA » de CERTIGNA sur son site ou sur le site d'une Autorité d'Enregistrement (AE) Externe ou Déléguée (AED), ainsi que les engagements et obligations respectifs des PARTIES liées aux présentes.

Les présentes CPU découlent d'une Politique de Certification (PC) associée aux CERTIFICATS délivrés. La PC est publiée en ligne et est identifiée par un identifiant unique OID dont découlent les OID des différents CERTIFICATS associés. Les CERTIFICATS couverts par les présentes CPU sont listés en Annexe 2 des présentes CPU.

2. CHAMP D'APPLICATION ET OPPOSABILITE

2.1. Champ d'application

Les présentes CGU s'appliquent aux CERTIFICATS délivrés par CERTIGNA par suite des DEMANDES DE CERTIFICATS effectuées sur le site internet de CERTIGNA accessible à l'adresse suivante : <https://www.certigna.com/> (le « Site »), ou sur le site d'une AE Externe ou Déléguée.

2.2. Opposabilité

Les présentes CGU deviennent opposables au PORTEUR dès l'instant où ils cochent la case prévue à cet effet. Ils reconnaissent alors en avoir eu connaissance et les avoir acceptées sans restriction ni réserve.

La confirmation de la DEMANDE DE CERTIFICATS vaut adhésion par le PORTEUR aux présentes CGU en vigueur au jour de la demande dont la conservation et la reproduction sont assurées par CERTIGNA conformément à l'article 1127-1 du code civil. Elles prévaudront sur toute autre version ou tout autre document contradictoire, ayant le même objet.

3. DÉFINITIONS

Les termes utilisés tout au long des présentes CPU, et écrit en majuscule ont, sauf stipulation contraire, la signification qui leur est donnée dans l'Annexe 1 aux présentes CPU qu'ils soient indifféremment utilisés au singulier ou au pluriel, ces définitions prévalant, pour ces seules CPU sur celles des CGU du Service de Vérification d'Identité en ligne et de Signature Electronique Avancée

4. LIVRAISON, GARANTIE ET CONFORMITÉ NORMATIVE

4.1. EMISSION ET DELIVRANCE DES CERTIFICATS

Tout CERTIFICAT commandé doit être accepté explicitement ou tacitement par le PORTEUR sur le compte client qu'il s'est créé depuis le Site ou depuis le site internet de l'une des AE Externes ou AED. Avant la génération du CERTIFICAT, Le PORTEUR doit vérifier que les informations énoncées dans la DEMANDE DE CERTIFICAT sont exactes. A défaut, le PORTEUR doit prendre contact avec un membre du personnel de l'AC, de l'AE Externe ou de l'AED. S'il s'agit de l'AC, soit par téléphone au 0 806 115 115 (service gratuit coût d'un appel local), soit par email à l'adresse suivante : contact@certigna.fr. Le support téléphonique est disponible du lundi au vendredi, sauf jours fériés, de 9h à 18h sans interruption. Le PORTEUR est conscient qu'en cas d'erreur lors de la DEMANDE DE CERTIFICAT dans la nature même du CERTIFICAT, aucune modification ne pourra être faite par l'AC et une nouvelle DEMANDE DE CERTIFICAT devra être réalisée par le PORTEUR. Si un paiement avait déjà été effectué, CERTIGNA ne serait tenue à aucun remboursement.

Le PORTEUR est amené à confirmer l'exactitude desdites informations avant ou après la génération du certificat. La confirmation de ces informations ou la première utilisation du CERTIFICAT vaut pour acceptation du CERTIFICAT.

A ce stade, aucune modification des informations ne peut être effectuée par l'AC. Il est donc de la responsabilité du PORTEUR de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le PORTEUR devra faire une nouvelle DEMANDE DE CERTIFICAT et le CERTIFICAT généré ne donnera lieu à aucun remboursement.

Une fois le CERTIFICAT accepté, celui-ci est utilisable par le PORTEUR en utilisant une donnée d'activation qui lui aura été communiquée par l'AC, l'AE ou l'AED (Ex : par mail ou SMS). L'utilisation du CERTIFICAT se fait sous la seule responsabilité

du PORTEUR via le site de l'AC, de l'AE Externe ou de l'AED. En cas de difficulté quelconque pendant cette dernière phase, le PORTEUR peut contacter l'AC, l'AE Externe ou l'AED au numéro de téléphone et l'adresse email de l'AC indiqués précédemment ou aux coordonnées disponibles sur le site de l'AE ou de l'AED. CERTIGNA ne garantit pas le fonctionnement du CERTIFICAT dans le cas d'une utilisation en dehors des usages prévus à l'article 8 des présentes.

4.2. CONFORMITE NORMATIVE DES CERTIFICATS

Le CERTIFICAT est émis en conformité avec les exigences de l'ETSI EN 319 411-1 pour le niveau LCP.

Les niveaux de qualifications et de certifications obtenus pour chaque CERTIFICAT sont décrits en Annexe 2 des présentes CGU.

5. DURÉE

Les CERTIFICATS émis par l'AC à destination des Porteurs ont une durée de validité de trente (30) minutes.

6. OBLIGATIONS DES PARTIES POUR LES CERTIFICATS

6.1 OBLIGATIONS DU PORTEUR

Le PORTEUR a le devoir de :

- Effectuer sa DEMANDE DE CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le Site de CERTIGNA, de l'AE Externe ou de l'AED ;
- Communiquer des informations exactes et à jour pour la DEMANDE DE CERTIFICAT ;
- Transmettre à l'AE, le cas échéant à l'AED, les informations requises pour la DEMANDE DE CERTIFICAT en ligne sur le Site ou sur le site de l'AE ou de l'AED le cas échéant, ainsi que les pièces justificatives.
- Accepter explicitement le CERTIFICAT avant ou après sa génération et depuis son compte client CERTIGNA ou celui de l'AE Externe ou de l'AED le cas échéant. Cette acceptation peut également être donnée implicitement par la première utilisation du CERTIFICAT.
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Respecter les conditions d'usages du CERTIFICAT et de la clé privée associée exposées à l'article 8 des présentes ;
- Ne plus utiliser un CERTIFICAT et la bi-clé associée à la suite de l'expiration ou la REVOCATION de ce CERTIFICAT ;
- Vérifier l'adéquation à son besoin du CERTIFICAT et de ses caractéristiques ;
- S'assurer que les prérequis matériels et/ou logiciels préconisés par l'AC sont remplis en vue de l'utilisation du CERTIFICAT ;
- Disposer de toutes les compétences et moyens nécessaires pour utiliser les CERTIFICATS.

6.2 OBLIGATIONS DE L'AC ET DE L'AE

CERTIGNA en tant qu'AC est tenue à une obligation de moyens pour toutes les obligations relatives à la gestion du cycle de vie du CERTIFICAT qu'elle émet. L'AC s'engage à :

- Pouvoir démontrer, aux UTILISATEURS, qu'elle a émis le CERTIFICAT pour un PORTEUR et que le PORTEUR correspondant a accepté le CERTIFICAT ;
- Prendre toutes les mesures raisonnables pour s'assurer que les PORTEURS sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des CERTIFICATS ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC ;
- Fournir un service de consultation en ligne sur le Site permettant à tout moment aux tiers de vérifier la validité du CERTIFICAT émis par l'AC (cf. article 9 des présentes) ;
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des CERTIFICATS non expirés.
- Réaliser toute collecte et tout usage de données à caractère personnel dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, et de la Politique d'utilisation des données personnelles disponible sur le Site de l'AC ;
- Mettre en œuvre et suivre, lors de l'émission d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC pour vérifier que les informations contenues dans le CERTIFICAT sont exactes ;

- Mettre en œuvre et suivre, lors de l'émission d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC pour vérifier l'identité du PORTEUR désigné, et ;
- Si l'AC et l'organisation qui demande le CERTIFICAT ne sont pas affiliées, ces parties s'engagent sur un accord de souscription juridiquement valide et exécutoire.

6.3 OBLIGATIONS DES UTILISATEURS DE CERTIFICATS

Les UTILISATEURS doivent :

- Respecter les usages autorisés du CERTIFICAT et de la clé privée associée. Dans le cas contraire, leur responsabilité pourrait être engagée ;
- Vérifier, avant son utilisation, l'état des CERTIFICATS de l'ensemble de la chaîne de certification correspondante via les moyens offerts pour la vérification des CERTIFICATS cités ci-dessous ; et
- Si le CERTIFICAT de l'AC racine CERTIGNA n'est pas installé sur le poste de l'UTILISATEUR, ce dernier doit le télécharger à partir du site <https://www.certigna.com> précisément aux adresses suivantes :
 - o <http://autorite.certigna.fr/tessica.der> ;
 - o <http://autorite.dhimyotis.com/tessica.der>.

Le CERTIFICAT de chaque Autorité de Certification CERTIGNA peut être téléchargé depuis les adresses suivantes :

TESSI SIGN CERTIFIED

- o <http://autorite.certigna.fr/tessisigncertified.der>
- o <http://autorite.dhimyotis.com/tessisigncertified.der>

7. PUBLICATION / REVOCATION DES CERTIFICATS

7.1 PUBLICATION

Le CERTIFICAT ne fait pas l'objet de publication par l'AC.

7.2 RÉVOCATION

Le CERTIFICAT du Porteur ne fait pas l'objet de révocation.

8. CONDITIONS D'USAGE DU CERTIFICAT ET DE LA CLÉ PRIVÉE ASSOCIÉE

Pour un CERTIFICAT de signature, les usages sont la signature électronique de données. Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

En cas de non-respect de ces usages, la responsabilité du PORTEUR pourrait être engagée dans les conditions prévues à l'article « Responsabilité du PORTEUR et de l'UTILISATEUR de CERTIFICAT » des présentes CGU.

9. VÉRIFICATION DES CERTIFICATS

Afin de vérifier la chaîne de certification, les UTILISATEURS (de CERTIFICATS peuvent télécharger les certificats d'autorités (AC RACINE et AC EMETTRICES) depuis le Site : <https://www.certigna.com>. Le CERTIFICAT d'AUTORITE RACINE peut être déjà installé sur le poste de travail de l'UTILISATEUR suivant la configuration logicielle de ce dernier. Afin de vérifier le statut de REVOCATION d'un CERTIFICAT, l'AC publie de façon périodique la LCR et offre un service d'information sur le statut de révocation des CERTIFICATS (serveur OCSP, pour On-line Certificate Status Protocol). Cette liste des CERTIFICATS révoqués et ces services sont accessibles pour les applications utilisant les CERTIFICATS aux adresses contenues dans les CERTIFICATS.

TESSI CERTIFIED CA

- Accès aux LCR <http://crl.certigna.fr/tessisigncertified.crl>
<http://crl.dhimyotis.com/tessisigncertified.crl>
- Accès à l'OCSP <http://tessisigncertified.ocsp.certigna.fr>
<http://tessisigncertified.ocsp.dhimyotis.com>

Dans le cadre de l'utilisation du service de répondeur OCSP de CERTIGNA, un nombre maximal de 250.000 requêtes OCSP est autorisé par CERTIFICAT et par jour. En cas de dépassement de ce seuil, CERTIGNA se réserve le droit d'imposer au PORTEUR du CERTIFICAT la mise en place du mécanisme d'OCSP Stapling sur le service utilisant le CERTIFICAT. En cas de refus de mise en place de l'OCSP stapling, CERTIGNA pourrait être amenée à révoquer le CERTIFICAT et ce, afin de maintenir et garantir la disponibilité du répondeur OCSP pour l'ensemble de ses clients.

10. RESPONSABILITÉ ET ASSURANCE

10.1. Responsabilité

En cas de manquement par le PORTEUR ou l'UTILISATEUR DE CERTIFICAT à leurs obligations respectives au titre des présentes CGU, leur responsabilité pourra être invoquée dans les conditions de droit commun.

La responsabilité de CERTIGNA ne pourra pas être recherchée pour tout préjudice indirect, tel que notamment, la perte de chiffre d'affaires, la perte de bénéfice, la perte de commandes, la perte de données, la perte d'une chance, le trouble à l'image ou tout autre dommage spécial ou événements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.

CERTIGNA ne saurait être tenue responsable de problèmes relevant de la force majeure, au sens du Code civil.

13.2. Assurance

CERTIGNA est titulaire d'une police d'assurance en matière de Responsabilité Civile Professionnelle, garantissant les dommages directs matériels ou immatériels consécutifs causés dans l'exercice de son activité professionnelle.

11. MODIFICATIONS DES CGU

Le PORTEUR convient que CERTIGNA pourra modifier les termes des présentes CPU unilatéralement et à tout moment. Toutefois, les conditions acceptées par le PORTEUR restent valides pendant toute la durée des CERTIFICATS délivrés sous couvert de ces conditions, sauf si le PORTEUR accepte explicitement les nouvelles conditions émises et publiées sur le Site de CERTIGNA, de l'AE Externe ou de l'AED. La nouvelle version des CGU s'appliquera à toute nouvelle DEMANDE DE CERTIFICAT.

12. DONNÉES PERSONNELLES

En acceptant les présentes CGU, le PORTEUR reconnaît avoir pris connaissance de [la Politique d'utilisation des Données Personnelles](#) de CERTIGNA disponible sur le Site.

Les données fournies par le PORTEUR lors de sa DEMANDE DE CERTIFICAT via le site de l'AC, de l'AE Externe ou de l'AED sont des Données Personnelles dont la collecte et le traitement sont régis par la Politique d'utilisation des Données Personnelles susvisée.

13. REGLEMENT DE CONFLITS

La validité des présentes CGU et toute autre question ou litiges relatifs à leur interprétation ou à leur exécution seront régis par le droit français.

Les PARTIES s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.

LES PARTIES CONVIENNENT, POUR LE CAS OU UN ACCORD AMIABLE SERAIT IMPOSSIBLE A ARRÊTER, QUE LES JURIDICTIONS COMPÉTENTES DU RESSORT DE LA COUR D'APPEL DE PARIS AURONT COMPÉTENCES EXCLUSIVES POUR CONNAÎTRE DE TOUT DIFFÉREND RESULTANT DE LA VALIDITÉ, DE L'INTERPRÉTATION, DE L'EXÉCUTION OU DE LA RESILIATION DES PRÉSENTES, ET PLUS GÉNÉRALEMENT DE TOUT LITIGE PROCÉDANT DES PRÉSENTES QUI POURRAIT LES DIVISER, NONOBTANT PLURALITÉS DES DÉFENDEURS OU APPEL EN GARANTIE.

14. COORDONNÉES DE LA SOCIÉTÉ CERTIGNA

CERTIGNA
SAS - RCS Lille n° 481463081
Zone de la plaine,
20 allée de la râperie 59493 Villeneuve d'Ascq
Tél : +33 806 115 115
Email : contact@certigna.com

15. SIGNALER UN CERTIFICAT MALVEILLANT OU DANGEREUX

Pour signaler un CERTIFICAT malveillant ou dangereux (un CERTIFICAT dont la clé privée est suspectée de compromission, un CERTIFICAT dont l'usage n'est pas respecté, ou tout autre type de fraude : compromission, détournement d'usage, conduite inappropriée, etc.) ou tout autre problème relatif aux CERTIFICATS, veuillez utiliser le formulaire de contact disponible à l'adresse suivante : <https://www.certigna.fr/contact.xhtml> et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

16. ENGAGEMENTS DE DISPONIBILITE RELATIFS AUX CERTIFICATS

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7 avec une durée d'indisponibilité maximale de la fonction définie par le tableau suivant :

Signature LCP

4 heures (jours ouvrés)	Par interruption (panne ou maintenance)
32 heures (jours ouvrés)	Par mois

ANNEXE 1: DEFINITIONS

Les termes énoncés ci-dessous, utilisés tout au long des présentes CGU, et débutant par une majuscule ont, sauf stipulation contraire, la signification suivante qu'ils soient indifféremment utilisés au singulier ou au pluriel :

- **AC** : Autorité de Certification de la société CERTIGNA, délivrant le CERTIFICAT.
- **AC RACINE** : Autorité de plus haut niveau de l'Infrastructure de Gestion de Clé (IGC) de CERTIGNA qui certifie les AC EMETTRICES.
- **AC EMETTRICE** : Autorité dont le CERTIFICAT a été signé par l'AC RACINE. L'AC est une autorité émettrice dans l'IGC CERTIGNA.
- **AE** : Autorité d'Enregistrement de la société CERTIGNA, contrôlant les demandes de CERTIFICAT des PORTEURS et ayant autorité pour demander la génération de CERTIFICATS auprès de l'AC ;
- **AE EXTERNE** : Entité tierce externe à l'IGC avec laquelle CERTIGNA a conclu un contrat de délégation par lequel il sous-traite toutes les activités de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des PORTEURS de CERTIFICAT et ayant autorité pour demander la génération de CERTIFICATS auprès de l'AC ;
- **AUTORITE D'ENREGISTREMENT DELEGUEE (AED)** : Entité tierce externe à l'IGC avec laquelle CERTIGNA a conclu un contrat de délégation par lequel il sous-traite une partie de l'activité de l'AE, à savoir, la collecte et le contrôle des dossiers d'enregistrement, l'identification des demandeurs de CERTIFICAT, la diffusion des CGU, l'affichage du contenu prévu ou présent dans le CERTIFICAT.
- **CERTIFICAT** : Certificat électronique constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations sur le PORTEUR.
- **COORDINATED UNIVERSAL TIME (UTC)** : Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-6.
- **DEMANDE DE CERTIFICAT** : Ensemble constitué du formulaire sur le site de l'AC, de l'AE Externe ou de l'AED

permettant de recueillir les informations nécessaires pour obtenir un CERTIFICAT (acceptant les présentes CGU) accompagné des pièces justificatives, et de la requête générée informatiquement.

- **INFRASTRUCTURE DE GESTION DE CLE (IGC)** : désigne l'ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, ...
- **LCR** : Liste des CERTIFICATS révoqués.
- **OCSP STAPLING** : Configuration du système de vérification de l'état du CERTIFICAT afin qu'il assure le rôle de proxy pour l'interrogation OCSP et cela afin de réduire drastiquement le nombre de requêtes transmises au répondeur OCSP de l'AC.
- **OID** : Identifiant d'objet (Object IDentifier).
- **PARTIE(S)** : Individuellement le PORTEUR et CERTIGNA
- **PORTEUR** : Personne physique pour laquelle la demande de CERTIFICAT a été acceptée et traitée par l'AC, qui est responsable de ce CERTIFICAT et de l'usage de la clé privée correspondante.
- **REVOCAION** : Opération consistant à mettre fin de manière anticipée à la durée de validité d'un CERTIFICAT initialement prévue et dont la date est inscrite dans le CERTIFICAT.
- **SUPPORT CRYPTOGRAPHIQUE** : dispositif au format clé USB ou carte à puce ou module cryptographique.
- **UTC(k)** : Temps de référence réalisé par le laboratoire "k" et synchronisé avec précision avec le temps UTC, dans le but d'atteindre une précision de ± 100 ns.
- **UTILISATEUR DE CERTIFICAT** : Pour un CERTIFICAT de signature, il peut s'agir :
 - o D'un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le PORTEUR du CERTIFICAT ;
 - o D'un usager qui signe électroniquement un document ou un message ;
 - o D'un usager destinataire d'un message ou de données et qui utilise un CERTIFICAT et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le PORTEUR du CERTIFICAT sur ce message ou sur ces données.



ANNEXE 2 : LISTE DES CERTIFICATS

Les CERTIFICATS couverts par les présentes CGVU sont les suivants :

TESSI SIGN CERTIFIED		ETSI	Profil
Signature	1.2.250.1.177.3.2.1	319 411-1 LCP	Porteur [Particulier]