1. OBJET

Les présentes conditions ont pour objet de préciser les conditions générales d'utilisation (CGU) des produits suivants délivrés par CERTIGNA sur le site https://www.certigna.com/ ainsi que les engagements et obligations respectifs des PARTIES liées aux présentes :

- **Les CERTIFICATS.** Pour les certificats, les CGU 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 le présent CONTRAT sont listés en **Annexe 2** des présentes CGU.
- **Les JETONS D'HORODATAGE** appelés également contremarques de temps. Pour les JETONS D'HORODATAGE, les CGU découlent d'une Politique de d'Horodatage (PH) associée aux JETONS D'HORODATAGE délivrés. Cette PH est identifiée par l'identifiant unique (OID) suivant : 1.2.250.1.177.2.9.1 et est publiée à l'adresse suivante : http://politique.certigna.fr/PHcertignaTSA.pdf

2. CHAMP D'APPLICATION ET OPPOSABILITE

2.1. Champ d'application

Les présentes CGU s'appliquent aux CERTIFICATS et JETONS D'HORODATAGE délivrés par CERTIGNA par suite des DEMANDES DE CERTIFICATS ou de JETONS D'HORODATAGE effectuées sur le site internet de CERTIGNA accessible à l'adresse suivante : https://www.certigna.com/ (le « **Site** »).

2.2. Opposabilité

Les présentes CGU deviennent opposables au DEMANDEUR, au PORTEUR, au RC et/ou au MANDATAIRE DE CERTIFICATION 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 ou JETONS D'HORODATAGE vaut adhésion par le DEMANDEUR, le PORTEUR, le RC et/ou le MANDATAIRE DE CERTIFICATION 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 CGU, et écrit en majuscule ont, sauf stipulation contraire, la signification qu'il leur ait donnée dans **l'Annexe 1** aux présentes CGU qu'ils soient indifféremment utilisés au singulier ou au pluriel.

4. LIVRAISON, GARANTIE ET CONFORMITÉ NORMATIVE

4.1. EMISSION ET DELIVRANCE DES CERTIFICATS

Tout CERTIFICAT commandé doit être accepté par le PORTEUR ou le RC sur le compte client qu'il s'est créé depuis le Site ou depuis le site internet de l'une des AED. Avant la génération du CERTIFICAT, Le DEMANDEUR, le PORTEUR ou le RC doit vérifier que les informations énoncées dans la DEMANDE DE CERTIFICAT sont exactes. A défaut, le DEMANDEUR, le PORTEUR ou le RC doit prendre contact avec un membre du personnel de l'AC 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 DEMANDEUR, le PORTEUR ou le RC est conscient qu'en cas d'erreur lors de la commande 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 DEMANDEUR, le PORTEUR ou le RC. Si un paiement avait déjà été effectué, CERTIGNA ne serait tenue à aucun remboursement.

Une fois la DEMANDE DE CERTIFICAT validée, le CERTIFICAT est généré. Le PORTEUR ou le RC est alors amené à confirmer l'exactitude desdites informations, ce qui vaut 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 ou du RC de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le PORTEUR ou le RC 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 mis à la disposition du PORTEUR ou du RC soit depuis son compte client, soit sur un SUPPORT CRYPTOGRAPHIQUE. L'installation du CERTIFICAT se fait sous la seule responsabilité du PORTEUR ou du RC. En cas de difficulté quelconque pendant cette dernière phase, le PORTEUR ou le RC peut contacter l'AC 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'AED. CERTIGNA ne garantit pas le fonctionnement du CERTIFICAT dans le cas d'une utilisation en dehors des usages prévus à l'article 9 des présentes.

4.2. CONFORMITE NORMATIVE DES CERTIFICATS

Le CERTIFICAT est émis en conformité avec un ou plusieurs des référentiels suivants :

- Les exigences de la PC Type « *Certificats électroniques de Services Applicatifs* » pour un usage de cachet ou d'authentification de client/serveur ou de la PC Type « *Certificats électroniques de Personnes* » pour un usage de chiffrement, d'authentification et/ou de signature du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Le règlement européen eIDAS (EU) N°910/2014 ;
- Les exigences de l'ETSI EN 319 411-1 niveau LCP, NCP, NCP+, DVCP, OVCP ou EVCP ;
- Les exigences de l'ETSI EN 319 411-2 niveau QCP, QCP-n, QCP-l, QCP-w, QCP-n-qscd or QCP-l-qscd;
- Les exigences du document « Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates » du CA/BROWSER FORUM.
- Les exigences du document « Guidelines For The Issuance and Management Of Extended Validation Certificates » du CA/BROWSER FORUM pour les CERTIFICATS d'authentification serveur qualifiés ;

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

4.3. CONFORMITE NORMATIVE DES JETONS D'HORODATAGE

Les JETONS D'HORODATAGE sont émis en visant la conformité avec les référentiels suivants :

- Les exigences de la « Politique d'horodatage type » du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Le règlement européen eIDAS (EU) N°910/2014 ;

- Les bonnes pratiques pour l'horodatage (BTSP) décrites dans l'ETSI EN 319 421 et identifiées par l'OID suivant : 0.4.0.2023.1.1

Les pratiques de services de confiance en vertu desquelles l'AC et l'AH opèrent sont non-discriminatoires.

5. DURÉE

Le CONTRAT est conclu pour l'une des durées suivantes :

Pour les CERTIFICATS, cette durée démarre le jour de la délivrance du CERTIFICAT par l'AC et ne peut excéder trois (3) ans sauf pour les CERTIFICATS d'authentification serveur et/ou client dont la durée ne peut excéder trois cent quatre-vingt-dix-huit (398) jours.

Pour les JETONS D'HORODATAGE, cette durée démarre le jour de la souscription au service d'HORODATAGE et ne peut excéder un (1) an. Cette durée est réinitialisée lors de toute nouvelle commande de JETONS D'HORODATAGE.

6. OBLIGATIONS DES PARTIES POUR LES CERTIFICATS

6.1 OBLIGATIONS DU DEMANDEUR

Le DEMANDEUR a le devoir de :

- Effectuer sa DEMANDE DE CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le Site.
- Communiquer des informations exactes, complètes et à jour pour la création de son compte client, la DEMANDE DE CERTIFICAT ou son renouvellement ;
- Confirmer que les informations à placer dans le CERTIFICAT sont correctes ;
- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de l'entité légale rattachée au CERTIFICAT, en main propre ou par voie postale (à ses frais), le formulaire d'inscription généré lors de la DEMANDE DE CERTIFICAT en ligne sur le Site ou sur le site de l'AED le cas échéant, le paiement, ainsi que les pièces justificatives ;
- Respecter les conditions d'usage du CERTIFICAT et de la clé privée associée exposées à l'article 9 des présentes et interdire toute utilisation non autorisée du CERTIFICAT et de la clé privée associée du PORTEUR, du service de CACHET ou du SERVEUR ;
- Générer le cas échéant, la bi-clé avec un modulus RSA de 2048 ou 3072 bits et en respectant les spécifications de l'ETSI 119 312 ;
- Générer le cas échéant, la bi-clé associée au CERTIFICAT dans un SUPPORT CRYPTOGRAPHIQUE qui est conforme aux exigences de sécurité du chapitre 11 de la Politique de Certification associée au CERTIFICAT.
  Des justificatifs attestant de la conformité du SUPPORT CRYPTOGRAPHIQUE pourront être demandés par l'AC lors de la DEMANDE DE CERTIFICAT (cas notamment d'un CERTIFICAT de CACHET). Ces justificatifs seront à minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé. **L'AC se réserve le droit de refuser la DEMANDE DE CERTIFICAT en l'absence de justificatifs ou s'il était avéré que ce dispositif ne réponde pas à ces exigences**.
- Maintenir la clé privée du PORTEUR sous son seul contrôle ;
- Maintenir la clé privée du service de CACHET ou SERVEUR sous le seul contrôle de la personne morale associée ;
- Informer sans délai l'AC de toute perte, vol ou compromission de la clé privée du PORTEUR, service de CACHET ou SERVEUR ;
- Informer sans délai l'AC si le contrôle de la clé privée du PORTEUR, du service ou SERVEUR a été perdu en raison de la compromission des données d'activation (par exemple, le code PIN) ou d'autres raisons ;
- Informer sans délai l'AC de toute modification concernant les informations contenues dans le CERTIFICAT ;
- Informer l'AE en cas de non-réception d'un e-mail confirmant la prise en compte de la DEMANDE DE CERTIFICAT ou de REVOCATION ;
- À la suite de la réception d'un e-mail de l'AE signalant la non-conformité de la DEMANDE DE CERTIFICAT ou que le dossier est incomplet, effectuer les modifications sous sept (7) jours calendaires après la réception dudit e-mail ;
- S'assurer que le CERTIFICAT du PORTEUR, du service de CACHET ou du SERVEUR n'est plus utilisé à la suite de l'expiration ou la REVOCATION de ce CERTIFICAT (Excepté pour les clés de chiffrement).
- Vérifier l'adéquation à son besoin du CERTIFICAT et de ses caractéristiques.

6.2 OBLIGATIONS DU PORTEUR OU DU RC

Le PORTEUR ou le RC a le devoir de :

- Effectuer sa DEMANDE DE CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le Site.
- Communiquer des informations exactes et à jour pour la DEMANDE DE CERTIFICAT ou son renouvellement ;
- Transmettre à l'AE, le cas échéant à l'AED, ou à un MC de l'entité légale rattachée au CERTIFICAT, en main propre ou par voie postale (à ses frais), le formulaire d'inscription généré lors de la DEMANDE DE CERTIFICAT en ligne sur le Site ou sur le site de l'AED le cas échéant, le paiement, ainsi que les pièces justificatives.
- Générer le cas échéant, la bi-clé avec un modulus RSA de 2048 ou 3072 bits et en respectant les spécifications de l'ETSI 119 312 ;
- Générer la bi-clé associée au CERTIFICAT dans un SUPPORT CRYPTOGRAPHIQUE qui est conforme aux exigences de sécurité du chapitre 11 de la Politique de Certification associée au CERTIFICAT.
  Des justificatifs attestant de la conformité du dispositif pourront être demandés par l'AC lors de la DEMANDE DE CERTIFICAT (cas notamment d'un CERTIFICAT de CACHET). Ces justificatifs seront à minima la facture d'achat du dispositif et des photos/impressions d'écran des caractéristiques matérielles et logicielles du dispositif et du numéro de série associé. **L'AC se réserve le droit de refuser la DEMANDE DE CERTIFICAT en l'absence de justificatifs ou s'il était avéré que ce dispositif ne réponde pas à ces exigences.**
- Dans le cas où l'AC serait informée de ou aurait identifié la perte de la conformité du dispositif, l'AC demandera au PORTEUR ou RC les preuves attestant que la bi-clé est toujours stockée dans un SUPPORT CRYPTOGRAPHIQUE répondant aux exigences du chapitre 11 de la Politique de Certification associée au CERTIFICAT. Le PORTEUR ou le RC s'engage à fournir ces preuves (Ex : facture d'achat d'un nouveau dispositif, procès-verbal de cérémonie des clés en cas de migration des clés, procès-verbal de mise à jour du dispositif pour le maintien de la certification, etc.) dans un délai de quinze (15) jours suivants la demande par l'AC. Dans le cas où aucune preuve ne serait fournie ou que les preuves ne permettraient pas de déterminer si les conditions de stockage de la bi-clé, et de transfert dans un autre dispositif

le cas échéant, répondent aux exigences de la Politique de Certification, l'AC se donne le droit de révoquer le CERTIFICAT.
- Informer l'AE en cas de non-réception d'un e-mail confirmant la prise en compte de la DEMANDE DE CERTIFICAT ou de REVOCATION ;
- À la suite de la réception d'un e-mail de l'AE signalant la non-conformité de la DEMANDE DE CERTIFICAT ou que le dossier est incomplet, effectuer les modifications sous sept (7) jours calendaires après la réception dudit e-mail ;
- Télécharger le CERTIFICAT généré, mis à disposition sur son compte client le cas échéant, dans les trente (30) jours qui suivent la validation de la DEMANDE DE CERTIFICAT qui est notifiée par e-mail au PORTEUR ou au RC. Au-delà de ce délai, le CERTIFICAT est révoqué automatiquement par l'AE.
- Accepter explicitement le CERTIFICAT après sa génération et depuis son compte client CERTIGNA ou celui de son AED le cas échéant. Cette acceptation peut également être opérée par l'envoi d'un courrier papier signé par le PORTEUR ou le RC sur demande expresse de l'AE. En cas de non-acceptation explicite, le CERTIFICAT est automatiquement révoqué par l'AE ;
- Protéger la clé privée associée au CERTIFICAT dont il a la responsabilité par des moyens appropriés à son environnement et conformément aux exigences du chapitre 11 de la Politique de Certification associée ;
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Protéger l'accès à la base de certificats du SERVEUR pour les CERTIFICAT d'authentification serveur/client ;
- Respecter les conditions d'usages du CERTIFICAT et de la clé privée associée exposées à l'article 9 des présentes ;
- Informer l'AC de toute modification concernant les informations contenues dans le CERTIFICAT ;
- Faire, sans délai, une demande de REVOCATION du CERTIFICAT dont il est responsable auprès de l'AE, de l'AED auprès de laquelle la DEMANDE DE CERTIFICAT a été effectuée ou le cas échéant du MC de l'entité légale rattachée au CERTIFICAT, lorsque l'une des causes de REVOCATION citées dans l'article 8.2 des présentes est rencontrée ;
- Prendre toutes les mesures propres à assurer la sécurité du ou des dispositifs sur lesquels est installé le CERTIFICAT. Le PORTEUR ou le RC est le seul responsable de l'installation du CERTIFICAT ;
- Ne plus utiliser un CERTIFICAT et à supprimer la bi-clé associée à la suite de l'expiration ou la REVOCATION de ce CERTIFICAT ;
- Informer l'AE de son départ de l'entité ou de son changement de responsabilités et du besoin d'enregistrer un nouveau PORTEUR ou RC ;
- 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'installation le cas échéant et de l'utilisation du CERTIFICAT ;
- Disposer de toutes les compétences et moyens nécessaires pour utiliser les CERTIFICATS ;
- Mettre en œuvre des mesures permettant d'empêcher toute personne non autorisée d'accéder physiquement au dispositif stockant la clé privée et le CERTIFICAT ;
- Prévenir sans délai la personne en charge de la sécurité des systèmes d'information de son entité (exemple : RSSI) en cas de perte ou de vol du dispositif stockant les clés et le CERTIFICAT ;
- Pour les applications jugées les plus critiques au niveau métier, mettre en place des mesures permettant de détecter des transactions potentiellement frauduleuses (incohérence des données métiers signées, etc.) et de prévoir, le cas échéant, une procédure alternative ; et
- S'il s'agit d'un CERTIFICAT d'authentification serveur et/ou client, et dans le cas où pour un ou plusieurs noms de domaine à intégrer dans le CERTIFICAT, l'option « DNS CAA » est activée, le RC doit mettre à jour les enregistrements DNS associés afin d'y faire figurer l'AC, et ce préalablement à la demande de CERTIFICAT.

6.3 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 ou un service de CACHET ou un SERVEUR donné et que le PORTEUR ou le RC correspondant a accepté le CERTIFICAT ;
- Prendre toutes les mesures raisonnables pour s'assurer que les PORTEURS et les RC 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 maintenance technique par téléphone aux heures ouvrées ;
- 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 11 des présentes) ;
- 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 ;
- 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 associée pour vérifier que l'organisation rattachée au PORTEUR ou au service de CACHET ou au SERVEUR a autorisé la délivrance du CERTIFICAT, et que le RC est autorisé à demander le CERTIFICAT au nom de l'organisation ;
- 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 de l'organisation, de son représentant légal et du PORTEUR ou RC désigné ;
- 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 ;
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des CERTIFICATS non expirés ; et
- Révoquer un CERTIFICAT pour l'une des raisons spécifiées à l'article 8.2 ;

- S'il s'agit d'un CERTIFICAT d'authentification serveur et/ou client, mettre en œuvre et suivre, lors de la délivrance d'un CERTIFICAT, les exigences décrites aux chapitres 3.2 et 3.3 de la PC associée pour vérifier que le PORTEUR ou le RC a le droit d'utiliser ou de contrôler le(s) nom(s) de domaine indiqué(s) dans les champs « commonName » et « subjectAltName » du CERTIFICAT (ou uniquement dans le cas où les droits d'utilisation ou de contrôle des noms de domaine ont été délégués par une personne disposant de ces droits) ;

CERTIGNA en tant qu'AE s'engage à :

- Vérifier et à valider les dossiers de DEMANDE DE CERTIFICAT et de REVOCATION de CERTIFICAT ;
- Générer et mettre à la disposition du PORTEUR ou du RC le CERTIFICAT dans un délai trente de (30) jours dans le cas où la DEMANDE DE CERTIFICAT est conforme et le dossier de demande complet ; et
- Révoquer le CERTIFICAT sous 24 heures dans le cas où la demande de REVOCATION est conforme et le demandeur est authentifié et autorisé.

6.4 OBLIGATIONS DES UTILISATEURS DE CERTIFCIATS

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 :
  - http://autorite.certigna.fr/ACcertignarootca.crt ;
  - http://autorite.dhimyotis.com/ACcertignarootca.crt.

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

CERTIGNA IDENTITY CA
http://autorite.certigna.fr/identca_rootca.crt
http://autorite.dhimyotis.com/identca_rootca.crt
CERTIGNA IDENTITY PLUS CA
http://autorite.certigna.fr/identityplusca_rootca.crt
http://autorite.dhimyotis.com/identityplusca_rootca.crt
CERTIGNA ENTITY CA
http://autorite.certigna.fr/entityca_rootca.crt
http://autorite.dhimyotis.com/entityca_rootca.crt
CERTIGNA ENTITY CODE SIGNING CA
http://autorite.certigna.fr/entitycsca_rootca.crt
http://autorite.dhimyotis.com/entitycsca_rootca.crt
FR03
http://autorite.certigna.fr/2ddoc.crt
http://autorite.dhimyotis.com/2ddoc.crt
CERTIGNA SERVICES CA
http://autorite.certigna.fr/servicesca.crt
http://autorite.dhimyotis.com/servicesca.crt
CERTIGNA WILD CA
http://autorite.certigna.fr/wildca.crt
http://autorite.dhimyotis.com/wildca.crt

7. OBLIGATIONS DES PARTIES POUR LES JETONS D'HORODATAGE

7.1 OBLIGATIONS DE L'ABONNÉ

L'ABONNÉ a le devoir d'émettre une requête utilisant un algorithme de hash supporté par l'AH (SHA256, SHA384 ou SHA512).

Il est recommandé que l'ABONNÉ, au moment de l'obtention d'un JETON D'HORODATAGE vérifie que le certificat de l'UNITE D'HORODATAGE n'est pas révoqué.

7.2 OBLIGATIONS DES UTILISATEURS DE JETONS D'HORODATAGE

Pour faire confiance à un JETON D'HORODATAGE, les UTILISATEURS doivent :

- Vérifier que le JETON D'HORODATAGE a été correctement signé, et que le certificat de l'UNITE D'HORODATAGE était valide au moment de la génération.
- Tenir compte des limitations sur l'utilisation du JETON D'HORODATAGE indiquées dans la POLITIQUE D'HORODATAGE et les présentes CGU.

7.3 OBLIGATIONS DE L'AH

L'AH assure tout ou partie de ces fonctions directement ou en les sous-traitant. Dans tous les cas, l'AH en garde la responsabilité. L'AH s'engage à respecter les obligations décrites dans la PH et veille à ce que ces exigences soient respectées. Elle s'engage également à ce que les composants de l'AH, internes ou externes à l'AH, auxquels elles incombent les respectent aussi. L'AH :

- garantit la conformité des exigences et des procédures prescrites dans la PH, même quand les fonctionnalités d'horodatage sont remplies par des sous-traitants ;
- garantit l'adhésion aux obligations complémentaires indiquées dans le JETON D'HORODATAGE ou bien directement ou bien incorporée par référence ;
- fournit le SERVICE D'HORODATAGE conformément à la PH et à la DPH associée ;
- remplit tous ses engagements tels que stipulés dans les présentes CGU.

8. PUBLICATION / REVOCATION DES CERTIFICATS

8.1 PUBLICATION

Le CERTIFICAT ne fait pas l'objet de publication par l'AC hormis s'il s'agit d'un CERTIFICAT de CACHET de documents de type 2D-DOC. Dans ce cas le RC accepte explicitement que le CERTIFICAT émis par l'AC fasse l'objet d'une publication dans un annuaire à l'adresse suivante : http://certificates.certigna.fr.

8.2 RÉVOCATION

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat par l'AC dans les vingt-quatre (24) heures :

- **La compromission de la clé** (RFC 5280 CRLReason #1) :
  - Le RC ou le Porteur, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat car il a raison de croire que la clé privée du certificat a été compromise, par exemple une personne non autorisée ayant eu accès à la clé privée du certificat ;
  - L'AC obtient la preuve que la clé privée correspondant à la clé publique du certificat est suspectée de compromission, est compromise,
  - L'AC est informée par une démonstration ou une méthode éprouvée que la clé privée est compromise ou il y une preuve évidente que la méthode spécifique pour générer

la clé privée était défectueuse. Des méthodes ont été développées qui peuvent aisément permettre de la calculer sur la base de la clé publique (telle que la clé vulnérable de Debian, cf. http://wiki.debian.org/SSLkeys).

- **Le retrait de privilège** (RFC 5280 CRLReason #9) :
  - L'AC obtient la preuve que l'usage du certificat est détourné
  - Le support cryptographique utilisé pour stocker le certificat et la clé privée du Porteur ou du RC n'est pas conforme ou ne sera plus conforme aux exigences du chapitre 11 de cette PC (Ex : une qualification ou certification ne serait plus maintenue ou serait suspendue) ;
  - L'AC est informée de tout changement dans les informations contenues dans le certificat ;
  - L'AC détecte ou est informée que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
  - Le représentant légal de l'entité à laquelle le service, le serveur ou le Porteur appartient le cas échéant, informe l'AC que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
  - L'AC est informée que le RC ou le Porteur n'a pas respecté toute ou partie des dispositions du contrat ou a violé une ou plusieurs de ses obligations en vertu des CGVU ;
  - L'AC est informée qu'un certificat Wildcard a été utilisé pour authentifier un FQDN subordonné frauduleusement trompeur.
- **L'arrêt des opérations** (RFC 5280 CLReason #5)
  - L'arrêt définitif du service ou serveur ou la cessation d'activité de l'entité du RC ;
  - Le départ de la société du Porteur ou la cessation d'activité de l'entité de rattachement du Porteur ;
  - Le RC n'a plus le contrôle ou n'est plus autorisé à utiliser les noms de domaines figurant dans le certificat ;
  - Le RC ne peut plus utiliser le certificat parce qu'il interrompt le site web ;
  - L'AC obtient la preuve que la validation de l'autorisation ou du contrôle d'un FQDN ou d'une adresse IP dans le certificat ne doit pas être jugée fiable ;
  - L'AC est informée de toute circonstance indiquant que l'utilisation d'un nom de domaine dans le certificat n'est plus autorisée légalement (Ex : un tribunal ou un arbitre a révoqué le droit d'un titulaire de nom de domaine d'utiliser le nom de domaine, une licence ou un accord de services entre le titulaire et le demandeur est terminée, ou le titulaire n'a pas pu renouveler le nom de domaine).
- **Le changement d'affiliation** (RFC 5280 CLReason #3)
  - Les informations du porteur, du service de cachet ou du serveur figurant dans le certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, modification de l'identité du porteur, du service de cachet ou du serveur), ceci avant l'expiration normale du certificat ;
  - Les informations figurant dans le registre public ont été modifiées de manière à influer considérablement sur la validité des attributs DSP2 du certificat ;
  - Le statut d'autorisation accordé par l'ACN a changé (par exemple, le PSP n'est plus autorisé).
- **Le remplacement ou l'annulation du certificat** (RFC 5280 CLReason #4)
  - Le RC ou le Porteur a demandé un nouveau certificat pour remplacer un certificat existant ;
  - L'AC obtient la preuve que la validation de l'autorisation du domaine ou du contrôle d'un ou plusieurs FQDN dans le certificat n'est pas fiable.
  - L'AC est informée que le certificat n'a pas été émis en conformité avec les exigences et pratiques formulées dans la PC ou la DPC associée ;
  - Le RC ou le Porteur, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC ;
  - Le certificat n'est plus conforme aux exigences des chapitres 6.1.5 et 6.1.6 de cette PC ;
- **Une autre raison de révocation qui résulte en l'absence d'extension « reasonCode » dans la CRL** :
  - Le RC, le Porteur, ou le représentant légal de l'entité à laquelle il appartient, demande par écrit, sans spécifier une raison de révocation, que l'AC révoque le certificat.
  - L'AC obtient la preuve que la clé privée correspondant à la clé publique du certificat est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
  - Le RC, le Porteur, ou le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée et/ou de son support) ;
  - Le droit de l'AC de délivrer des certificats sous les exigences du CA/Browsers Forum expire ou est révoqué ou terminé, à moins que l'AC ait prévu de continuer le maintien des services de CRL/OCSP ;
  - La révocation est requise par cette PC ou la DPC correspondante pour une raison qui ne nécessite pas d'être spécifiée dans ce présent chapitre ;
  - L'AC cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC assure le relai en cas de révocation du certificat ;
  - Le certificat de signature de l'AC est révoqué, ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante ;
  - Le contenu ou le format des certificats présente un risque inacceptable pour les fournisseurs de logiciels applicatifs ou les utilisateurs (Ex : le CA/Browser Forum peut déterminer qu'un algorithme ou une clé de chiffrement/signature obsolète présente un risque inacceptable et que ces certificats doivent être révoqués et remplacés par l'AC sous un délai donné.
  - Une erreur (intentionnelle ou non) a été détectée dans la demande de certificat et le dossier d'enregistrement correspondant ;
  - Pour des raisons techniques (échec de l'envoi du certificat, ...).

La demande de REVOCATION peut être effectuée par :

- Le PORTEUR ou le RC, un représentant légal de l'entité rattachée au CERTIFICAT, ou le cas échéant un MC de cette entité, et/ou
- L'AC, l'AE ou un AED.

La demande de REVOCATION peut être effectuée :

- Par courrier signé, accompagné de la photocopie d'une pièce d'identité officielle du demandeur ;

- En ligne, sur le Site ou le site de l'AED, depuis l'espace client du PORTEUR ou du RC ou du MC le cas échéant.

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

- Pour un CERTIFICAT de chiffrement, les usages sont :
  - Déchiffrement : à l'aide de sa clé privée, un PORTEUR déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique figurant dans le CERTIFICAT ;
  - Chiffrement : à l'aide de la clé publique du destinataire, une personne chiffre des données.
- Pour un CERTIFICAT d'Authentification et/ou de signature, les usages sont :
  - Authentification des PORTEURS auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.
  - 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.
- Pour un CERTIFICAT de cachet pour la signature de mails et de documents, les usages sont la signature électronique de données et la vérification de signature électronique. Ces données peuvent être, par exemple, un accusé de réception à la suite de la transmission d'informations par un usager à un service applicatif, une réponse automatique à une demande formulée par un usager, un mail, un document ou encore une archive.
- Pour un CERTIFICAT de cachet pour la signature de JETONS D'HORODATAGE, les usages sont la signature électronique de JETONS D'HORODATAGE et la vérification de signature électronique.
- Pour un CERTIFICAT de cachet de documents 2D-DOC, les usages sont la signature électronique de données contenues dans un 2D-DOC et la vérification de la signature électronique. Le type de données signées doit être conforme à celui qui a été déclaré par le RC lors de la DEMANDE DE CERTIFICAT.
- Pour un CERTIFICAT d'Authentification serveur et/ou client, les usages sont l'authentification du SERVEUR auprès d'autres SERVEURS ou de personnes, dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS ou IPsec visant à établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

En cas de non-respect de ces usages, la responsabilité du PORTEUR ou du RC ou de l'entité à laquelle le CERTIFICAT est rattaché pourrait être engagée.

10. EXACTITUDE ET LIMITE D'UTILISATION DES JETONS D'HORODATAGE

L'AH garantit que son horloge est synchronisée avec le temps UTC selon une exactitude d'une seconde.

Les JETONS D'HORODATAGE peuvent être vérifiés à minima 2 ans après leur génération.

Les JETONS D'HORODATAGE ne sont pas conservés et archivés par l'AH.

11. VÉRIFICATION DES CERTIFICATS

Afin de vérifier la chaîne de certification, les UTILISATEURS (de CERTIFICATS ou de JETONS D'HORODATAGE) ou les ABONNES 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.

CERTIGNA IDENTITY CA	
Accès aux LCR	http://crl.certigna.fr/identca.crl http://crl.dhimyotis.com/identca.crl
Accès à l'OCSP	http://identca.ocsp.certigna.fr http://identca.ocsp.dhimyotis.com
CERTIGNA IDENTITY PLUS CA	
Accès aux LCR	http://crl.certigna.fr/identityplusca.crl http://crl.dhimyotis.com/identityplusca.crl
Accès à l'OCSP	http://identityplusca.ocsp.certigna.fr http://identityplusca.ocsp.dhimyotis.com
CERTIGNA ENTITY CA	
Accès aux LCR	http://crl.certigna.fr/entityca.crl http://crl.dhimyotis.com/entityca.crl
Accès à l'OCSP	http://entityca.ocsp.certigna.fr http://entityca.ocsp.dhimyotis.com
CERTIGNA ENTITY CODE SIGNING CA	
Accès aux LCR	http://crl.certigna.fr/entitycsca.crl http://crl.dhimyotis.com/entitycsca.crl
Accès à l'OCSP	http://entitycsca.ocsp.certigna.fr http://entitycsca.ocsp.dhimyotis.com
FR03	
Accès aux LCR	http://crl.certigna.fr/2ddoc.crl http://crl.dhimyotis.com/2ddoc.crl
Accès à l'OCSP	http://2ddoc.ocsp.certigna.fr http://2ddoc.ocsp.dhimyotis.com
CERTIGNA SERVICES CA	
Accès aux LCR	http://crl.certigna.fr/servicesca.crl http://crl.dhimyotis.com/servicesca.crl
Accès à l'OCSP	http://servicesca.ocsp.certigna.fr http://servicesca.ocsp.dhimyotis.com
CERTIGNA WILD CA	
Accès aux LCR	http://crl.certigna.fr/wildca.crl http://crl.dhimyotis.com/wildca.crl
Accès à l'OCSP	http://wildca.ocsp.certigna.fr http://wildca.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 ou au RC 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.

12. RESPONSABILITÉ ET ASSURANCE

12.1. **Responsabilité**

CERTIGNA est soumise à une obligation générale de moyens. CERTIGNA ne pourra voir sa responsabilité engagée à l'égard du DEMANDEUR, du PORTEUR, du RC ou de l'ABONNE que pour les dommages directs qui pourraient lui être imputés au titre des produits et services délivrés dans le cadre du CONTRAT.

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 évènements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.

CERTIGNA n'est responsable que des tâches expressément mises à sa charge dans le cadre du CONTRAT.

CERTIGNA ne saurait être tenue responsable de quelque manière que ce soit de l'utilisation faite par le PORTEUR, le RC du CERTIFICAT, l'ABONNE ou un UTILISATEUR, ni du contenu des documents et des données qui lui sont remis par le PORTEUR, le RC, le DEMANDEUR ou l'ABONNE.

En aucun cas, la responsabilité de CERTIGNA ne saurait être recherchée pour :

- Faute, négligence, omission ou défaillance du DEMANDEUR, du PORTEUR du RC ou de l'ABONNE, qui constituerait la cause exclusive de survenance du dommage ;
- Dysfonctionnement ou d'indisponibilité d'un bien matériel ou immatériel dans le cas où celui-ci a été fourni par le PORTEUR, le RC ou l'ABONNE ;
- Retard dans la fourniture des données à traiter dû au DEMANDEUR, au PORTEUR, au RC ou à l'ABONNE ;
- Perte de la qualification d'un tiers prestataire qui est indépendant de la volonté de CERTIGNA (Ex : le fournisseur du SUPPORT CRYPTOGRAPHIQUE du CERTIFICAT ou de celui utilisé pour le CERTIFICAT d'une UH).

De convention expresse entre les PARTIES, la responsabilité de CERTIGNA est limitée, tous préjudices confondus, à la somme de deux (2) fois le montant réglé par le client au titre des produits et services délivrés. CERTIGNA n'est responsable que des tâches expressément mises à sa charge dans le cadre du CONTRAT.

CERTIGNA ne pourra être tenue responsable d'une utilisation non autorisée ou non conforme des JETONS D'HORODATAGE délivrés par son SERVICE D'HORODATAGE.

CERTIGNA ne sera en aucun cas responsable des éventuels dommages ayant leur origine dans l'utilisation d'un JETON D'HORODATAGE délivré par l'AH.

CERTIGNA ne pourra pas être impliquée pour des retards ou pertes que pourraient subir les données transmises sur lesquelles est demandé un JETON D'HORODATAGE par le service applicatif.

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

Les données transmises dans une requête d'horodatage et la vérification de leur valeur dans la réponse associée restent de la responsabilité de l'ABONNÉ.

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.

13. MODIFICATIONS DES CGU

Le DEMANDEUR, le PORTEUR, le RC ou l'ABONNE convient que CERTIGNA pourra modifier les termes des présentes CGU unilatéralement et à tout moment. Toutefois, les conditions acceptées et signées par le DEMANDEUR, le PORTEUR, le RC ou l'ABONNE restent valides pendant toute la durée des CERTIFICATS ou JETONS D'HORODATAGE délivrés sous couvert de ces conditions, sauf si le DEMANDEUR, le PORTEUR, le RC ou l'ABONNE accepte explicitement les nouvelles conditions émises et publiées sur le Site. La nouvelle version des CGU s'appliquera à toute nouvelle demande de produits sur le Site.

14. DONNÉES PERSONNELLES

En acceptant les présentes CGU, le DEMANDEUR, le PORTEUR, le RC ou l'ABONNE reconnaît avoir pris connaissance de la Politique d'utilisation des Données Personnelles de CERTIGNA disponible sur le Site.

Les données fournies par le DEMANDEUR, le PORTEUR, le RC ou l'ABONNE, lors de son inscription sur le Site et lors de sa DEMANDE DE CERTIFICAT ou de JETON D'HORODATAGE sont des Données Personnelles dont la collecte et le traitement sont régis par la Politique d'utilisation des Données Personnelles susvisée.

15. 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 ARRETER, QUE LES JURIDICTIONS COMPETENTES DU RESSORT DE LA COUR D'APPEL DE PARIS AURONT COMPETENCES EXCLUSIVES POUR CONNAITRE DE TOUT DIFFEREND RESULTANT DE LA VALIDITE, DE L'INTERPRETATION, DE L'EXECUTION OU DE LA RESILIATION DES PRESENTES, ET PLUS GENERALEMENT DE TOUT LITIGE PROCEDANT DES PRESENTES QUI POURRAIT LES DIVISER, NONOBSTANT PLURALITES DES DEFENDEURS OU APPEL EN GARANTIE.

16. 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

17. 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 ».

18. PERTE DE QUALIFICATION/CERTIFICATION DU SUPPORT

22.1 Le SUPPORT CRYPTOGRAPHIQUE, délivré le cas échéant par CERTIGNA au PORTEUR ou au RC pour stocker et utiliser la clé privée et le CERTIFICAT, bénéficie d'une ou plusieurs qualifications et/ou certifications. Dans le cas où l'une de ces qualifications ou certifications ne serait plus maintenue ou suspendue pour des raisons telles que l'identification d'une vulnérabilité ou l'arrêt de fabrication du produit, CERTIGNA en informera le PORTEUR ou le RC et révoquera son CERTIFICAT, sans condition de remboursement.

22.2 Le SUPPORT CRYPTOGRAPHIQUE, utilisé le cas échéant par CERTIGNA pour stocker et utiliser la clé privée et le CERTIFICAT d'une UH, bénéficie d'une ou plusieurs qualifications et/ou certifications. Dans le cas où l'une de ces qualifications ou certifications ne serait plus maintenue ou suspendue pour des raisons telles que l'identification d'une vulnérabilité ou l'arrêt de maintenance du produit, CERTIGNA en informera l'ABONNÉ et révoquera le CERTIFICAT, sans condition de remboursement sur les JETONS D'HORODATAGE émis préalablement avec ce CERTIFICAT.

19. 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 :

RGS ***	
2 heures	Par interruption (panne ou maintenance)
8 heures	Par mois
RGS **	
4 heures	Par interruption (panne ou maintenance)
16 heures	Par mois
RGS *	
4 heures (jours ouvrés)	Par interruption (panne ou maintenance)
32 heures (jours ouvrés)	Par mois

La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7 pour les révocations en ligne avec une durée d'indisponibilité maximale de la fonction définie par le tableau suivant :

RGS ***	
1 heure	Par interruption (panne ou maintenance)
4 heures	Par mois
RGS **	
2 heures	Par interruption (panne ou maintenance)
8 heures	Par mois
RGS *	
2 heures (jours ouvrés)	Par interruption (panne ou maintenance)
16 heures (jours ouvrés)	Par mois

20. ENGAGEMENTS DE SERVICES POUR L'OPTION PREMIUM HORODATAGE

Engagement de disponibilité :

Certigna s'engage sur un taux de disponibilité de 99.9%, étant précisé qu'une indisponibilité sera le résultat d'un incident critique défini comme l'interruption complète du service d'horodatage.

Le taux de disponibilité annuelle sera calculé sur la base de 12mois de 30 jours de 24heures, et au prorata temporis pour le mois de mise en service et pour le mois de résiliation du service.

Seuls les incidents critiques de responsabilité Certigna sont pris en compte dans le cadre du calcul de la disponibilité annuelle :

- Disponibilité = MTBF / (MTTI + MTBF)

Moyenne Temps Bon Fonctionnement = Somme des Temps de Bon Fonctionnement / nombre d'incidents critiques de défaillances

Moyenne Temps Total des Indisponibilités = Temps d'arrêt total / nombre incidents critiques

Pénalité associée :

Dans le cas de non atteinte de l'engagement de disponibilité, les pénalités suivantes seront applicables :

Déficit de disponibilité	**Pénalité** **Exprimée en % de la moyenne mensuelle de la facturation annuelle (abonnement + consommation de jetons)**
Inférieur à 0,01%	3%
De 0,01% à 0,02%	4%
Au-delà de 0,03%	5%

Centre de Services :

La déclaration d'un incident devra se faire sur l'adresse mail astreinte@certigna.com

21. 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 :

- **ABONNÉ** : Personne morale ou personne physique ayant besoin de faire horodater des données par l'AUTORITE D'HORODATAGE et qui a accepté les présentes CGU.
- **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 et les éventuelles demandes de REVOCATION.
- **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 et la soumission des demandes de REVOCATION.
- **AUTORITÉ D'HORODATAGE (AH)** : Autorité d'horodatage de la société CERTIGNA en charge du SERVICE D'HORODATAGE en conformité avec la POLITIQUE D'HORODATAGE et en s'appuyant sur une ou plusieurs UNITES D'HORODATAGE.
- **CACHET** : Des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières.

- **CERTIFICAT** : Certificat électronique constitué d'un fichier de données électroniques signé numériquement, conforme à la norme X.509 v3, contenant des informations :
  - sur le SERVEUR dont est responsable le RC pour un CERTIFICAT d'authentification serveur et/ou client ;
  - sur le service de CACHET dont est responsable le RC pour un CERTIFICAT de CACHET ;
  - sur le PORTEUR pour un CERTIFICAT de chiffrement ou d'authentification et/ou de signature.
- **CONTRAT** :
  - Pour les CERTIFICATS : relations entre CERTIGNA et le PORTEUR ou le RC qui sont encadrées par les présentes CGU expressément acceptées par le PORTEUR ou le RC lors de chaque DEMANDE de CERTIFICAT.
  - Pour les JETONS D'HORODATAGE : relations entre CERTIGNA et l'ABONNÉ encadrées par les présentes CGU expressément acceptées par l'ABONNÉ lors de la commande de JETONS D'HORODATAGE.

  Sont également inclus dans le CONTRAT l'ensemble des documents auxquels les présentes CGU font référence notamment la Politique d'utilisation des données personnelles disponible sur le site Certigna.com.
- **COORDINATED UNIVERSAL TIME (UTC)** : Echelle de temps liée à la seconde, telle que définie dans la recommandation ITU-R TF.460-6.
- **DEBLOCAGE** : Opération consistant à réinitialiser le code PIN d'un **SUPPORT CRYPTOGRAPHIQUE** bloqué à la suite de la saisie de 3 codes PIN incorrects ;
- **DEMANDE DE CERTIFICAT** : Ensemble constitué du formulaire de demande signé (acceptant les présentes CGU) accompagné des pièces justificatives, et de la requête générée informatiquement.
- **DEMANDEUR** : Personne physique demandant un certificat :
  - **pour lui-même** : dans ce cas il est tenu de respecter les obligations de demandeur (chapitre 6) ainsi que de PORTEUR ou RC (chapitre 7) ; ou
  - **au nom et pour le compte du PORTEUR**. Dans ce cas il est tenu de respecter les obligations de demandeur uniquement (chapitre 6) ; les obligations du PORTEUR restant à la charge de ce dernier
- **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, ...
- **JETON D'HORODATAGE** : Donnée signée électroniquement qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là.
- **LCR** : Liste des CERTIFICATS révoqués.
- **MANDATAIRE DE CERTIFICATION (MC)** : Personne physique désignée par et placée sous la responsabilité de l'entité légale rattachée au CERTIFICAT. Elle est en relation directe avec l'AE et assure pour elle un certain nombre de vérifications concernant l'identité du PORTEUR ou du RC de cette entité.
- **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 DEMANDEUR, le PORTEUR, le RC ou l'ABONNÉ ou CERTIGNA, et collectivement, CERTIGNA et le DEMANDEUR, CERTIGNA et le PORTEUR, CERTIGNA et le RC ou CERTIGNA et l'ABONNÉ.
- **POLITIQUE D'HORODATAGE (PH)** : Ensemble de règles qui indique l'applicabilité d'un JETON D'HORODATAGE à une communauté particulière et/ou à une catégorie d'application avec des exigences de sécurité commune.
- **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 la clé privée correspondante.
- **RC** : Personne physique en charge et responsable du CERTIFICAT utilisé pour le SERVEUR ou le service de CACHET et de la clé privée associée.
- **REFABRICATION** : Opération consistant à émettre un nouveau CERTIFICAT en remplacement d'un existant, avec exactement les mêmes informations mais une bi-clé différente (à la suite de la perte du certificat ou du mot de passe).
- **REVOCATION** : 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.
- **SERVEUR** : serveur informatique hébergeant un service sécurisé par un CERTIFICAT, permettant l'authentification de ce service par des UTILISATEURS et la sécurisation des échanges avec ces derniers.
- **SERVICE D'HORODATAGE :** Ensemble des prestations nécessaires à la génération et à la gestion de JETONS D'HORODATAGE.
- **SUPPORT CRYPTOGRAPHIQUE** : dispositif au format clé USB ou carte à puce ou module cryptographique.
- **UNITE D'HORODATAGE (UH)** : Ensemble de matériels et de logiciels en charge de la création de JETONS D'HORODATAGE caractérisé par un identifiant de l'UNITE D'HORODATAGE accordé par une AC, et une clé unique de signature de JETONS D'HORODATAGE. Les UNITES D'HORODATAGE de l'AH utilisent des CERTIFICATS de CACHET d'horodatage émis par l'AUTORITE DE CERTIFICATION « Certigna Entity CA ». Ces CERTIFICATS ont un nom ayant la syntaxe suivante « CERTIGNA – TSU <N° de la TSU> ».
- **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 JETON D'HORODATAGE** : Entité (personne ou système) qui fait confiance à un JETON D'HORODATAGE émis sous la POLITIQUE D'HORODATAGE.
- **UTILISATEUR DE CERTIFICAT** : Il peut s'agir de :
  - ABONNÉ ou UTILISATEUR DE JETONS D'HORODATAGE.
  - Pour un CERTIFICAT de chiffrement, il peut s'agir d'un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du PORTEUR du CERTIFICAT, ou encore d'une personne qui émet un message chiffré à l'intention du PORTEUR du CERTIFICAT.
  - Pour un CERTIFICAT d'Authentification, il peut s'agir :

- D'un service en ligne qui utilise un CERTIFICAT et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le PORTEUR du CERTIFICAT dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le PORTEUR du CERTIFICAT ;
- D'un usager destinataire d'un message ou de données et qui utilise un CERTIFICAT et un dispositif de vérification d'authentification afin d'en authentifier l'origine.

- Pour un CERTIFICAT de signature, il peut s'agir :
  - 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 ;
  - D'un usager qui signe électroniquement un document ou un message ;
  - 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.
- Pour un CERTIFICAT d'Authentification **et** de signature, il peut s'agir des mêmes UTILISATEURS que pour un CERTIFICAT d'authentification ou un CERTIFICAT de signature.
- Pour un CERTIFICAT de CACHET, il peut s'agir :
  - Un usager destinataire de données signées par un service applicatif de CACHET et qui utilise le CERTIFICAT ainsi qu'un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.
  - Un service applicatif destinataire de données provenant d'un autre service applicatif et qui utilise le CERTIFICAT et un module de vérification de CACHET afin d'authentifier l'origine de ces données transmises.
  - Un service applicatif qui signe des données électroniques.
- Pour un CERTIFICAT d'Authentification de SERVEUR, il peut s'agir d'une personne accédant à un SERVEUR et qui utilise le CERTIFICAT du SERVEUR et un module de vérification d'authentification afin d'authentifier le SERVEUR auquel il accède, qui est identifié dans le CERTIFICAT du SERVEUR, afin d'établir une clé de session partagée entre son poste et le SERVEUR ;
- Pour un CERTIFICAT d'Authentification client, il peut s'agir d'un service applicatif accédant à un SERVEUR et qui utilise un CERTIFICAT et un applicatif de vérification d'authentification afin d'authentifier le SERVEUR auquel il accède, qui est identifié dans le CERTIFICAT, et afin d'établir une clé de session partagée entre les deux SERVEURS.

ANNEXE 2 : LISTE DES CERTIFICATS

Les CERTIFICATS couverts par les présentes CGVU sont les suivants :

CERTIGNA ENTITY CA	**1.2.250.1.177.2.6.1**	**RGS**	**ETSI**	**Profil**
Cachet de documents	1.2.250.1.177.2.6.1.1.1	RGS *	LCP	RC
Cachet de documents	1.2.250.1.177.2.6.1.1.2	RGS *	LCP	RC
Cachet de documents	1.2.250.1.177.2.6.1.4.1	RGS **	QCP-l-qscd	RC
Cachet de documents	1.2.250.1.177.2.6.1.4.2	RGS **	QCP-l-qscd	RC
Cachet de documents	1.2.250.1.177.2.6.1.42.1	RGS **	LCP	RC
Cachet de documents	1.2.250.1.177.2.6.1.42.2	RGS **	LCP	RC
Cachet de documents	1.2.250.1.177.2.6.1.41.1		QCP-l-qscd	RC
Cachet de documents	1.2.250.1.177.2.6.1.41.2		QCP-l-qscd	RC
Cachet de documents	1.2.250.1.177.2.6.1.7.1		QCP-l	RC
Cachet de documents	1.2.250.1.177.2.6.1.7.2		QCP-l	RC
Cachet de documents	1.2.250.1.177.2.6.1.8.1		QCP-l + PSD2	RC
Cachet de documents	1.2.250.1.177.2.6.1.8.2		QCP-l + PSD2	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.9.1		QCP-l	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.9.2		QCP-l	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.3.1	RGS *	LCP	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.3.2	RGS *	LCP	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.6.1	RGS **	QCP-l-qscd	RC
Cachet de jetons d'horodatage	1.2.250.1.177.2.6.1.6.2	RGS **	QCP-l-qscd	RC
CERTIGNA ENTITY CODE SIGNING CA	**1.2.250.1.177.2.8.1**	**RGS**	**ETSI**	**Profil**
Cachet de code	1.2.250.1.177.2.8.1.1.1	RGS *	LCP	RC
Cachet de code	1.2.250.1.177.2.8.1.1.2	RGS *	LCP	RC
Cachet de code	1.2.250.1.177.2.8.1.2.1	RGS **	QCP-l-qscd	RC
Cachet de code	1.2.250.1.177.2.8.1.2.2	RGS **	QCP-l-qscd	RC
FR03	**1.2.250.1.177.2.2.1**	**RGS**	**ETSI**	**Profil**
Cachet de documents (2D-DOC)	1.2.250.1.177.2.2.1.1	RGS *	LCP	RC
CERTIGNA SERVICES CA	**1.2.250.1.177.2.5.1**	**RGS**	**ETSI**	**Profil**
Authentification serveur	1.2.250.1.177.2.5.1.1.1	RGS *	OVCP	RC
Authentification serveur	1.2.250.1.177.2.5.1.1.2	RGS *	OVCP	RC
Authentification client	1.2.250.1.177.2.5.1.2.1	RGS *	OVCP	RC
Authentification client	1.2.250.1.177.2.5.1.2.2	RGS *	OVCP	RC
Authentification serveur/client	1.2.250.1.177.2.5.1.3.1		QEVCP-w	RC
Authentification serveur/client	1.2.250.1.177.2.5.1.4.1		QEVCP-w	RC
Authentification serveur/client	1.2.250.1.177.2.5.1.4.2		QEVCP-w	RC
Authentification serveur/client	1.2.250.1.177.2.5.1.5.1		QNCP-w	RC
Authentification serveur/client	1.2.250.1.177.2.5.1.5.2		QNCP-w	RC
CERTIGNA WILD CA	**1.2.250.1.177.2.7.1**	**RGS**	**ETSI**	**Profil**
Authentification client/serveur	1.2.250.1.177.2.7.1.1.1		OVCP	RC
Authentification client/serveur	1.2.250.1.177.2.7.1.1.2		OVCP	RC
Authentification client/serveur wildcard	1.2.250.1.177.2.7.1.2.1		OVCP	RC
Authentification client/serveur wildcard	1.2.250.1.177.2.7.1.2.2		OVCP	RC
CERTIGNA IDENTITY CA	**1.2.250.1.177.2.3.1.**	**RGS**	**ETSI**	**Profil**
Chiffrement	1.2.250.1.177.2.3.1.1.1	RGS *	LCP	PORTEUR
Chiffrement	1.2.250.1.177.2.3.1.1.2	RGS *	LCP	PORTEUR
Chiffrement	1.2.250.1.177.2.3.1.3.1	RGS *	LCP	PORTEUR
Chiffrement	1.2.250.1.177.2.3.1.3.2	RGS *	LCP	PORTEUR
Authentification & signature	1.2.250.1.177.2.3.1.2.1	RGS *	LCP	PORTEUR
Authentification & signature	1.2.250.1.177.2.3.1.2.2	RGS *	LCP	PORTEUR
Authentification & signature	1.2.250.1.177.2.3.1.4.1	RGS *	LCP	PORTEUR
Authentification & signature	1.2.250.1.177.2.3.1.4.2	RGS *	LCP	PORTEUR

CERTIGNA IDENTITY PLUS CA	1.2.250.1.177.2.4.1.	RGS	ETSI	Profil
Authentification & signature	1.2.250.1.177.2.4.1.1.1	RGS **	QCP-n-qscd	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.1.2	RGS **	QCP-n-qscd	PORTEUR
Authentification	1.2.250.1.177.2.4.1.2.1	RGS ***	NCP+	PORTEUR
Authentification	1.2.250.1.177.2.4.1.2.2	RGS ***	NCP+	PORTEUR
Signature	1.2.250.1.177.2.4.1.3.1	RGS ***	QCP-n-qscd	PORTEUR
Signature	1.2.250.1.177.2.4.1.3.2	RGS ***	QCP-n-qscd	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.4.1	RGS **	QCP-n-qscd	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.4.2	RGS **	QCP-n-qscd	PORTEUR
Authentification	1.2.250.1.177.2.4.1.5.1	RGS ***	NCP+	PORTEUR
Authentification	1.2.250.1.177.2.4.1.5.2	RGS ***	NCP+	PORTEUR
Signature	1.2.250.1.177.2.4.1.6.1	RGS ***	QCP-n-qscd	PORTEUR
Signature	1.2.250.1.177.2.4.1.6.2		QCP-n-qscd	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.7.1		QCP-n	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.7.2		QCP-n	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.8.1		QCP-n-qscd	PORTEUR
Authentification & signature	1.2.250.1.177.2.4.1.8.2		QCP-n-qscd	PORTEUR