

# Conditions Générales d'Utilisation

## ChamberSign France CA3 Qualified eID

### QCP-n-qscd\_double\_usage



<b>Objet du document :</b>	Ce document décrit les conditions générales d'utilisation des certificats émis par l'Autorité de Certification mise en œuvre par ChamberSign France dans le cadre de ses activités de services de confiance.
<b>Version</b>	02
<b>Date de diffusion</b>	17/12/2021
<b>Type de diffusion</b>	Public

## Avertissement

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1<sup>er</sup> juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de **CHAMBERSIGN FRANCE**. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par **CHAMBERSIGN FRANCE** ou ses ayants droit, sont strictement interdites.

A juste titre, aux termes de l'article L.122-4 du Code de la Propriété Intellectuelle, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause est illicite* ».

Par exception, le Code de la Propriété Intellectuelle autorise, aux termes de l'article L.122-5 dudit Code, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » ; d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

La représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Le présent document, propriété de **CHAMBERSIGN FRANCE**, peut être concédé par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.



## 1. Préambule

1. Chambersign France est une association régie par la loi du 1<sup>er</sup> juillet 1901, enregistrée sous le numéro SIREN 433 702 479, dont le siège social est situé 8-10 rue Pierre Brossolette 92300 LEVALLOIS PERRET.
2. ChamberSign France met à la disposition du Client et de son Représentant Légal, du Porteur, du Mandataire de Certification et de l'Utilisateur du Certificat des services de certification.
3. Toute utilisation des services proposés suppose la consultation et l'acceptation sans réserve des Conditions Générales.
4. Le Client, son Représentant Légal, le Porteur, le Mandataire de Certification et l'Utilisateur du Certificat reconnaissent avoir lu, compris et approuvé les CGU ainsi que la Politique de certification (ci-après « PC ») du Certificat dont l'OID est 1.2.250.1.96.1.8.2.8, acceptent pleinement leur contenu et reconnaissent être liés par la totalité de leurs dispositions.
5. Le Client, son Représentant Légal, le Porteur, le Mandataire de Certification et l'Utilisateur du Certificat reconnaissent disposer de la compétence et des moyens nécessaires pour utiliser les Certificats.
6. Le Client, son Représentant Légal, le Porteur, le Mandataire de Certification et l'Utilisateur du Certificat reconnaissent avoir pris connaissance de la nature, de la destination et des modalités d'utilisation des Certificats et avoir sollicité et obtenu les informations nécessaires pour utiliser les Certificats en toute connaissance de cause.
7. Dans la mesure du possible et selon l'état d'avancement des technologies, ChamberSign France travaille à adapter ses services de certification aux personnes handicapées.

## 2. Définitions

8. Les termes ci-dessous définis auront entre les parties la signification suivante :
  - « **Application Utilisatrice** » : désigne les services applicatifs utilisant des Certificats émis par ChamberSign France pour des besoins d'authentification et de signature du Porteur ;
  - « **Authentification** » : désigne le processus ayant pour but de vérifier l'identité dont se réclame une personne ou une machine (ci-après désignée « Entité ») ;
  - « **Autorité de Certification** » ou « **AC** » : au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ « issuer » du certificat), dans les certificats émis au titre de cette politique de certification. Cette entité est responsable de l'émission, de la délivrance, de la gestion et de la révocation des certificats électroniques. Elle est également responsable des certificats émis en son nom. ChamberSign France est une Autorité de Certification qualifiée RGS et eIDAS. Elle a fait l'objet d'un contrôle de conformité par l'Agence Nationale de la Sécurité des Systèmes d'Information et est inscrite sur la liste de confiance européenne ;
  - « **Autorité d'Enregistrement Déléguée** » ou « **AED** » : désigne une entité publique ou privée, composante d'une Autorité de Certification, responsable de l'identification du porteur et de la délivrance de certificats électroniques ;



- « **Bi-clé** » : désigne un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique correspondante, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. La clé publique permet de vérifier les signatures électroniques par la clé privée associée. La clé publique est scellée avec l'identité du signataire dans le certificat électronique associé ;

- « **Bureau d'Enregistrement** » ou « **BE** » : désigne le service mis en place par une CCI signataire d'une convention avec l'AC ayant pour objet de procéder à l'enregistrement de porteur (vérification du dossier, réalisation de face à face et remise de support de clé) et à la révocation. La collecte et la vérification des informations sont nécessaires à la délivrance d'un certificat ;

- « **Cachet serveur** » : désigne une signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non-répudiation dans le cadre d'échanges dématérialisés ;

- « **Certificat électronique** » : désigne un ensemble d'informations d'un utilisateur, y compris la clé publique, rendu infalsifiable par le chiffrement, avec la clé secrète de l'AC qui l'a délivré, d'un condensat calculé sur l'ensemble de ces informations. Un certificat contient des informations telles que :

- l'identité du porteur de certificat ;
- la clé publique du porteur de certificat ;
- usage(s) autorisé(s) de la clé ;
- la durée de vie du certificat ;
- l'identité de l'AC qui l'a émis ;
- la signature de l'AC qui l'a émis.

Un format standard de certificat est défini dans la recommandation X.509 v3.

Dans le monde numérique, un certificat est l'équivalent d'une pièce d'identité, en ce sens qu'il est porteur d'une identité certifiée par une Autorité de Certification. Le certificat électronique comporte les éléments attestant du lien entre les données de vérification de signature et l'identité du signataire ;

- « **Clé Privée** » : désigne une clé mathématique que le Porteur doit conserver secrètement ;

- « **Clé Publique** » : désigne une clé mathématique rendue publique et qui est utilisée pour vérifier la signature d'une donnée reçue ;

- « **Client** » : désigne l'Entité qui contracte avec ChamberSign France pour bénéficier d'un Certificat. Toute obligation applicable au Client s'applique également à son Représentant Légal, au Mandataire de Certification et au Porteur ;

- « **Compromission** » : désigne la divulgation ou suspicion de divulgation ou de perte d'informations confidentielles résultant de la violation d'une mesure de sécurité et conduisant à une possible perte de confidentialité et/ou d'intégrité des données considérées. Il peut s'agir également de l'altération ou de la suspicion d'altération de la qualité d'un certificat électronique au sens de l'article 33 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique ;

- « **Conditions Générales** » ou « **CGU** » : désigne les présentes conditions générales d'utilisation ;



- « **Déléataire** » : désigne une personne nommément désignée par le Représentant Légal d'une Entité lui transférant l'exercice de commander des certificats électroniques pour le compte d'une autre personne via une délégation de signature transmise à ChamberSign ;
- « **Données Confidentielles** » : désigne ensembles la Clé Privée du Certificat, le code de retrait et le code d'activation de la Clé Privée, qui sont des données strictement personnelles au Porteur qui devront être impérativement gardées secrètes ;
- « **Données à caractère personnel** » : désigne toute information relative à une personne physique identifiée ou identifiable ;
- « **Entité** » : désigne toute autorité administrative ou entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations ;
- « **Infrastructure de Gestion des Clés** » ou « **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 autorité de certification, 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, etc ;
- « **LAR** » : désigne la liste des Certificats d'Autorité de Certification révoqués ;
- « **LCR** » : désigne la liste des certificats révoqués ;
- « **Mandataire de Certification** » : désigne la personne désignée par le Représentant Légal du Client aux fins de recueillir les pièces des dossiers de demande de Certificats, de réaliser la reconnaissance en face à face avec les Porteurs et d'effectuer les demandes de Révocation des Certificats ;
- « **OID** » : désigne le numéro d'identifiant objet désignant la Politique de Certification de l'Autorité de Certification ;
- « **Politique de Certification** » ou « **PC** » : désigne l'ensemble des règles et exigences, identifiées par un OID, auxquelles ChamberSign France se conforme dans le cadre des présentes et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes ;
- « **Porteur** » : désigne la personne physique identifiée dans le Certificat et qui est le détenteur de la Clé Privée correspondant à la Clé Publique qui est dans ce Certificat ;
- « **Prestataire de services de certification électronique** » ou « **PSCE** » désigne toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ « issuer » du certificat ;
- « **Règlement eIDAS** » : désigne le Règlement européen qui s'applique à l'identification électronique, aux services de confiance et aux documents électroniques, et abroge la directive 1993/03/CE sur la signature électronique. Il impose des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique ainsi qu'à celle des



signatures électroniques, pour les échanges entre les organismes du secteur public et les usagers ;

- « **Représentant Légal** » : désigne le représentant légal du Client ;
- « **Responsable de certificat** » : désigne la personne en charge et responsable du certificat électronique de type cachet ou d'authentification serveur ;
- « **Révocation du certificat** » : désigne l'action qui a pour but l'extinction de la validité du Certificat. Un Certificat qui a fait l'objet d'une Révocation est inscrit sur la LCR ;
- « **RGPD** » : désigne le Règlement Général sur la Protection des Données, (règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données), et abrogeant la Directive 95/36/CE ;
- « **RGS** » : désigne un référentiel documentaire réalisé par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) qui définit des exigences pour différentes fonctions de sécurité. Il concerne les produits de sécurité et les prestataires de services de confiance utilisés dans le cadre des échanges dématérialisés entre usagers et autorités administratives ainsi qu'entre autorités administratives. Les niveaux de sécurité d'exigences sont croissants (\*, \*\*, \*\*\*) et comportent des spécifications techniques différentes (source site internet de l'ANSSI) ;
- « **Signature Electronique** » : désigne l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache, conformément à la législation applicable ;
- « **Site** » : désigne le site Internet <https://www.chambersign.fr/>, propriété de ChamberSign ;
- « **Tiers archiveur** » : désigne une organisation ou une personne morale ou physique qui se charge pour le compte de tiers de gérer et d'assurer la conservation de ses archives.
- « **Utilisateur du Certificat** » : désigne l'entité ou la personne physique qui reçoit un document ou une transaction ayant utilisé un Certificat et qui s'y fie pour vérifier une valeur d'authentification ou une signature électronique provenant du Porteur.

### 3. Objet

9. Les CGU ont pour objet de définir les conditions selon lesquelles le Client pourra utiliser les Certificats tels que définis à l'article « Définitions » des présentes CGU et émis par ChamberSign France en tant qu'Autorité de Certification, conformément à sa Politique de Certification.

### 4. Contact

10. Toute demande peut être adressée à :

- ChamberSign France – Immeuble Le Cours de Midi, 10 cours de Verdun Rambaud 69002 LYON ;
- [qualite@chambersign.fr](mailto:qualite@chambersign.fr)

## **5. Durée – Entrée en vigueur - Opposabilité**

11. Les CGU sont opposables au Client et au Porteur dès leur signature et, à défaut de signature, dès la première utilisation du Certificat qui implique l'acceptation pleine et entière des nouvelles CGU par le Client. Le Client se porte-fort du respect des CGU par l'Utilisateur du Certificat.

12. Les CGU sont conclues et opposables pendant toute la durée de vie du Certificat, d'une période de trois (3) ans, renouvelable à la demande du Client une fois et pour une période de trois (3) ans, sous réserve des dispositions légales et réglementaires, sans préjudice de leurs éventuelles mises à jour et modifications que ChamberSign France s'engage à communiquer au Client par tous moyens à sa disposition (courrier électronique, information en ligne, etc.).

13. Toute utilisation du Certificat après les modifications ou la mise à jour des CGU vaut acceptation pleine et entière des nouvelles CGU par le Client.

14. La dernière version des CGU est également disponible sur le site web de ChamberSign France. Elles peuvent être adressées à première demande par courrier électronique.

## **6. Demande de certificats et renouvellement**

### **6.1. Enregistrement des dossiers de demande de certificat**

15. Le Porteur, le Représentant Légal du Client, ainsi que le Mandataire de Certification peuvent faire une demande de Certificat en remplissant le formulaire de demande de Certificat sur le site Internet de ChamberSign France : [www.chambersign.fr](http://www.chambersign.fr).

16. Les pièces justificatives à joindre lors d'une demande initiale de Certificat sont précisées dans le Contrat d'abonnement.

17. Le Client doit envoyer les pièces justificatives nécessaires par un courrier, un moyen électronique sécurisé ou les présenter directement au BE.

### **6.2. Vérification de la demande**

18. Le BE réalise les opérations suivantes :

- vérifie et valide l'identité du futur Porteur ;
- vérifie la cohérence des justificatifs présentés ;
- s'assure que le futur Porteur a pris connaissance des CGU, des modalités applicables pour l'utilisation du Certificat et a accepté les CGU.

19. L'identité du Porteur est vérifiée au travers de la vérification de documents officiels d'identité effectuée lors d'un face à face.

20. Les fichiers de demande de certificat, contenant la clé publique à certifier, sont scellés à l'aide de la clé privée correspondante.

21. Les informations concernant la structure à laquelle le porteur est rattaché font l'objet de vérifications lors de l'enregistrement (existence, validité...).

### **6.3. Rejet de la demande**

22. En cas de pièces manquantes et après relance quant à la communication de ces pièces, le BE se réserve le droit de rejeter la demande de Certificat.

23. Il en informe le Porteur, le Mandataire de Certification ou le Représentant Légal du Client.

### **6.4. Délivrance du certificat**

24. Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC, le processus consiste à remettre au Porteur en mains propres un support cryptographique vierge, identifié de façon unique et lié au Porteur, qui fera l'objet d'une personnalisation sous le contrôle du Porteur : personnalisation du code d'activation (code PIN), génération de la bi-clé dans le support, envoi de la clé publique à la fonction de génération des certificats, téléchargement sur le support du certificat généré.

25. Le futur Porteur peut aussi utiliser un support cryptographique qu'il détient déjà pour d'autres certificats ChamberSign délivrés à son nom. Le BE vérifiera que ce support est conforme, au moment du face à face de délivrance, au niveau de qualification requis pour la génération de la Bi-clé du nouveau certificat et le contrôle exclusif de la clé (Code PIN). La décision d'accepter ou de refuser le support par le BE est sans appel.

26. Les certificats sont émis conformément au profil défini dans le document [GUI.ACC.11].

27. Après authentification de l'origine et vérification de l'intégrité de la demande provenant du BE, ChamberSign France génère le Certificat, la Bi-clé du Porteur, son dispositif d'authentification et de signature, les codes d'activation et tous autres éléments nécessaires au bon fonctionnement du Certificat, ce que le Porteur accepte.

28. La disponibilité des Certificats émis par ChamberSign France à l'issue de la procédure d'enregistrement donne lieu à l'émission d'un avis de mise à disposition sous forme de message électronique à l'attention du Porteur qui devra suivre les indications décrites pour en effectuer le retrait.

29. Chaque demande de Certificat fait l'objet d'un face à face du Porteur avec un BE, un agent de l'AED, un représentant de ChamberSign France ou un Mandataire de Certification.

30. Les clés privées des Porteurs, générées dans le dispositif cryptographique du Porteur, ne sont pas exportables et ne font donc l'objet d'aucun séquestre ni d'aucune sauvegarde.

31. Les supports cryptographiques des Porteurs font l'objet d'une qualification par l'ANSSI au niveau requis par le règlement [eIDAS] et le règlement [RGS].

32. Les supports cryptographiques contenant les clés privées des Porteurs ne sont activés qu'après la saisie d'un code d'activation (code PIN) entièrement maîtrisé par le Porteur et qu'il doit garder secret. Les supports cryptographiques contenant les clés privées des porteurs doivent assurer la fonction d'authentification ou de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers

33. Les données d'activation correspondent aux codes PIN des supports cryptographiques, qui sont définis par les Porteurs lors de la personnalisation de leur support et qui doivent rester sous leur contrôle exclusif. Les différentes composantes de l'IGC n'ont à aucun moment connaissance de ces données.





34. Le retrait des supports physiques vierges et la génération des Certificats s'effectuent auprès du BE, de l'AED, du Mandataire de Certification ou auprès d'une personne désignée par ChamberSign France, dans les deux mois suivant la réception du message informant le Porteur de la mise à disposition du Certificat.

35. ChamberSign France se réserve le droit de ne pas donner suite à la procédure de délivrance du Certificat si le Porteur ne s'est pas présenté pour retirer son Certificat deux mois après ledit message.

## **6.5. Acceptation du certificat**

36. Suite à son retrait, le Porteur doit tester son Certificat au moyen du service prévu à cet effet sur le site internet de ChamberSign France ou par ses propres moyens.

37. Le certificat fait l'objet d'une acceptation explicite par le Porteur au moment de sa remise.

38. Le Porteur accepte son Certificat en signant électroniquement avec celui-ci un document d'acceptation, en ligne.

39. Le Porteur procède aussi à la signature électronique de sa commande et aux CGU du certificat si ces deux documents n'ont pas été signés physiquement.

40. Toute demande de modification du Certificat nécessite pour le Porteur d'effectuer une nouvelle demande de Certificat.

## **6.6. Assistance**

41. Afin d'accompagner le Porteur, une notice technique d'utilisation du Certificat est disponible sur le site internet de ChamberSign France et une assistance téléphonique est mise à sa disposition au 08 92 23 02 52 depuis la France métropolitaine (tarif en vigueur ou accessible sur le site internet de ChamberSign France) de 9 heures à 12h30 heures et de 13h30 à 18h sauf le vendredi à 17h00, les jours ouvrés.

42. Un tutoriel ainsi qu'une foire aux questions sont disponibles sur le site internet de ChamberSign France à l'adresse suivante : <https://www.chambersign.fr>.

## **6.7. Renouvellement**

43. La cause principale de la délivrance d'un nouveau certificat et de la bi-clé correspondante est la fin de validité du certificat. La durée de validité des certificats ChamberSign France est de trois (3) ans. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaques cryptographiques.

44. Un renouvellement peut être aussi réalisé de manière anticipée, suite à un événement ou un incident déclaré par le Porteur, les plus fréquents étant la perte, le vol ou le dysfonctionnement du support cryptographique. Dans ce cas, le renouvellement consiste pour le Porteur à refaire une demande initiale.

45. Une modification des informations contenues dans le certificat entraîne également la délivrance d'un nouveau certificat (avec renouvellement de la bi-clé).



46. La délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale.

47. Le renouvellement d'un Certificat en fin de validité implique le renvoi des pièces justificatives qui ne sont plus valables ou qui ont subi des modifications, conformément au Contrat d'abonnement. Tout Porteur est averti par message électronique de l'arrivée à expiration de son Certificat. S'il souhaite le renouveler, il formule une demande de renouvellement avant la date d'expiration sur le site Internet de ChamberSign France.

48. Le renouvellement d'un Certificat implique un renouvellement de la Bi-clé correspondante et un changement des dates de validité mais non des autres informations qui restent identiques au précédent Certificat.

49. En cas de déqualification du support physique du Certificat pendant sa période de validité initiale, notamment due à un changement de PC ou de réglementation, le renouvellement du Certificat pourra être effectué uniquement sur un nouveau support physique qualifié au bon niveau de sécurité.

### **6.8. Modification du certificat**

50. La modification d'un Certificat correspond à des modifications d'informations sans changement de la Clé Publique. ChamberSign France ne procède à aucune modification de Certificat.

51. En cas de modification des informations contenues dans le Certificat, le Certificat devra être révoqué et une nouvelle demande de Certificat devra être faite, selon les modalités définies par les CGU.

### **6.9. Déblocage du certificat / Perte du mot de passe**

52. En cas de blocage du Certificat, notamment dû à une erreur de code PIN, tout déblocage devra être fait par l'intermédiaire de ChamberSign France uniquement ou de ses BE.

53. Toute demande de déblocage devra être précédée de l'installation du logiciel Java sur l'ordinateur du Porteur.

54. Toute tentative de déblocage effectuée directement par le Client ou le Porteur, via le logiciel pilote, pourrait donner lieu à un dysfonctionnement du support physique du Certificat à la charge du Client.

## **7. Conditions d'usage des certificats et limites**

55. Les usages sont :

- la signature électronique de données ou de documents par le Porteur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, l'identification du signataire.
- l'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.



56. L'authentification ne constitue pas une signature au sens juridique du terme, car elle ne signifie pas que le porteur manifeste son consentement sur les données échangées (la garantie de non-répudiation n'est donc pas offerte).

57. Pour information, le recours à un certificat double-usage peut introduire une faille de sécurité potentielle. Cette faille de sécurité dépend notamment de l'environnement mis en œuvre par le Porteur de Certificat.

58. Si l'environnement du Porteur est sous son contrôle et est de confiance, alors il n'y a pas d'impacts sécurité particuliers à prendre en compte.

59. En revanche, si l'environnement utilisé n'est pas réputé sûr, il appartient au Porteur de s'assurer que l'opération qu'il est en train de faire est bien une opération d'authentification ou bien une opération de signature. Le Porteur doit avoir conscience qu'il est possible d'utiliser son certificat pour réaliser une signature en lieu et place d'une authentification et réciproquement.

60. Dans le cas où l'environnement du Porteur n'est pas réputé sûr, il est recommandé qu'il s'assure d'une part que la clé privée n'est utilisée que pour le certificat double-usage qui lui a été émis, et d'autre part que l'application mettant en œuvre les mécanismes d'authentification ou de signature utilise les bons usages du certificat.

61. L'utilisation de la Clé Privée du Porteur et du Certificat doit rester strictement limitée aux services d'Authentification et de Signature électronique.

62. Il est possible d'utiliser le Certificat à des fins non-professionnelles, sauf interdiction du Client envers le Porteur.

63. En tout état de cause, le Client est pleinement responsable vis-à-vis de ChamberSign France de l'utilisation du Certificat faite par le Porteur.

64. Par ailleurs, ChamberSign France peut être amenée à émettre des certificats de test. Ces certificats de test sont identifiés comme tels dans leur DN par la mention explicite « TEST ». Ils ne sont couverts par aucune garantie par ChamberSign France et ils ne doivent en aucun cas être utilisés à d'autres fins qu'à des fins de test. A la fin des phases de tests, ces certificats sont révoqués. Lesdits certificats de test ne contiennent aucune donnée à caractère personnel.

## **8. Procédure de vérification des certificats**

65. Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :

- la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du Porteur lui-même) ;
- les informations ou les attributs du Porteur figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;
- les algorithmes cryptographiques mis en œuvre sont obsolètes et ne sont plus considérés sûrs ;
- il a été démontré que le Porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;



- le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ;
- le Porteur ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès).

66. Les causes de révocation ne sont jamais publiées.

67. ChamberSign France s'engage à mettre à disposition, 24h/24, un service de consultation sur son site internet [www.chambersign.fr](http://www.chambersign.fr) permettant de vérifier la validité des Certificats qu'elle a émis.

68. Les informations mises à disposition de l'Utilisateur du Certificat par ChamberSign lui permettent de vérifier et de valider, préalablement à son utilisation, le statut d'un Certificat et de l'ensemble de la chaîne de Certification correspondante.

69. Chambersign France publie dans sa Politique de Certification les exigences qu'elle met en œuvre afin de respecter la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat.

## 9. Révocation du certificat

70. Un Certificat sera révoqué pour les causes suivantes :

- modification d'une information contenue dans le Certificat ;
- informations inexactes fournies dans le dossier d'enregistrement ;
- non-paiement du prix du Certificat par le Client, échéance initiale ou ultérieure en cas de paiement échelonné ;
- compromission possible ou avérée de la Clé Privée du Porteur ;
- dysfonctionnement du support physique ;
- non-respect par le Porteur des règles d'utilisation du Certificat ou des présentes CGU ;
- non-respect par le Porteur ou le Client de la PC de ChamberSign France ;
- réalisations d'opérations frauduleuses ;
- résiliation de l'abonnement ;
- demande de révocation du Certificat par le Client ;
- cessation de l'activité du Porteur au sein du Client et ce, quelle qu'en soit la cause : décès, démission... ;
- vol ou perte du support physique du Certificat physique ou perte du mot de passe pour un certificat logiciel ;
- cessation d'activité du Client.



71. Une demande de révocation du Certificat pourra être faite à tout moment par lettre recommandée avec demande d'avis de réception auprès du BE ou par remise en mains propres au BE, ou bien en ligne à partir du site Internet à l'adresse suivante : [www.chambersign.fr](http://www.chambersign.fr) ou, pour le Représentant Légal, depuis le site Internet à l'adresse suivante : <https://viseo.chambersign.fr/auth/login.jsf>.

72. Dans le cas d'une délivrance d'un certificat électronique réalisée depuis la nouvelle plateforme de Viseo via l'Espace Client (<https://viseo3.chambersign.fr/#/accueil>) et délivré au moyen d'une attestation de face à face signée par le Porteur [FOR.ACC.21], la demande de révocation en ligne se réalisera également sur ce même Espace, en cliquant directement sur le lien suivant : <https://viseo3.chambersign.fr/#/espace-revocation>.

73. La demande de révocation peut émaner des personnes suivantes :

- le Représentant Légal du Client ;
- le Porteur du Certificat ;
- le Mandataire de Certification ;
- ChamberSign France.

74. En cas de vol ou de perte du support physique et lorsque plusieurs Certificats sont stockés sur ce même support, la demande de révocation du Porteur devra porter sur l'ensemble de ces Certificats.

75. Toute demande de révocation fait l'objet d'une authentification du demandeur et d'une vérification de son autorité.

76. La demande de révocation fait l'objet d'une procédure de vérification des informations relatives au demandeur et de son autorité par rapport au Certificat.

77. Le Porteur reçoit une confirmation par e-mail de cette révocation. Une fois le certificat révoqué, le Porteur s'interdit expressément d'utiliser la Clé Privée et le Certificat.

78. Le Porteur reconnaît et accepte qu'il supportera l'entière responsabilité de toute utilisation du Certificat après avoir eu connaissance de la survenance d'un des événements susmentionnés, sans préjudice de toute action en responsabilité que ChamberSign France se réserve le droit d'exercer contre le Porteur.

79. Toute période d'abonnement, annuelle ou triennale entamée, est due dans son intégralité et ce, quel que soit la cause de révocation des certificats ou de de résiliation de l'abonnement.

80. Il n'y a pas de suspension possible de certificat. Seule la révocation définitive des certificats peut être réalisée.

81. ChamberSign France assure la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat en mettant en œuvre les mesures suivantes :

- Publication sans limite de temps des certificats révoqués dans les LCR publiées. La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7.

82. La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de deux (2) heures ;



83. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de huit (8) heures.

## **10. Obligations de Chambersign**

84. ChamberSign France attribue à sa PC un OID qui est porté dans les Certificats correspondants qu'elle s'engage à faire évoluer en cas d'évolution significative de sa PC.

85. ChamberSign France s'engage au contrôle par le BE de l'identification du Porteur, du Représentant Légal et le cas échéant, du Mandataire de Certification se présentant pour obtenir un Certificat.

86. ChamberSign France s'engage à réaliser les prestations de Certification selon les modalités et dans les limites des CGU.

87. ChamberSign France s'engage à démontrer à l'Utilisateur du Certificat qui en fait la demande qu'elle a émis un Certificat pour un Porteur donné et que ce Porteur a accepté le Certificat.

88. ChamberSign France s'engage à tout mettre en œuvre pour créer et émettre des Certificats contenant des informations réputées exactes.

89. Pour cela, ChamberSign France s'engage à s'assurer que le dossier de demande de Certificat est complet, que les pièces fournies sont apparemment conformes.

90. ChamberSign France s'engage à ce que le Certificat soit prêt à la délivrance pour le Porteur dans un délai de quarante-huit (48) heures à compter de la remise d'un dossier complet au BE.

91. ChamberSign France s'engage à établir, par l'émission d'un Certificat, un lien entre l'identité d'une personne et les informations contenues dans ledit Certificat.

92. Dans l'hypothèse où le Représentant Légal du Client aurait recours aux services d'un Délégué, le BE s'engage à effectuer le contrôle de l'identité du Délégué et la vérification de l'existence du contrat de mandat entre le Représentant Légal du Client et le Délégué.

93. Le Délégué sera tenu de s'assurer de la validité du mandat qui lui a été conféré par le Client ou son Représentant Légal.

94. ChamberSign France prend toutes les mesures raisonnables pour s'assurer que les Porteurs sont au courant de leurs droits et obligations concernant l'utilisation et la gestion des clés, des Certificats et de l'équipement et des logiciels utilisés aux fins de l'IGC.

95. ChamberSign France prend les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la PC.

96. ChamberSign France a un devoir général de surveillance quant à la sécurité et l'intégrité des Certificats délivrés par elle-même ou l'une de ses composantes.

97. ChamberSign France s'engage sur le bon fonctionnement des Certificats qu'elle délivre.

## 11. Obligations du Client

98. Le Client et son Représentant Légal s'engagent à respecter les stipulations des présentes CGU.

99. Le Client et son Représentant Légal sont responsables de la gestion des Certificats délivrés aux employés, Délégués ou agents du Client dans le cadre du contrat d'abonnement de façon expresse, et s'engage à faire en sorte que tout Porteur de Certificat respecte les obligations prévues par les présentes CGU et qu'aucune fraude ou erreur n'est commise. A ce titre, le Client et son Représentant Légal s'assurent notamment que le Porteur :

- communique les informations utiles à la création du Certificat et les éventuelles modifications pendant toute la durée du Certificat ;
- respecte la procédure de révocation décrite à l'article « Révocation du Certificat » des présentes CGU ;
- conserve secrètes et de manière sécurisée les données confidentielles et le support physique du Certificat.

100. Le Client et son Représentant Légal s'engagent à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des Certificats.

101. Le Client et son Représentant Légal s'engagent à informer le BE de rattachement de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, sans délais. ChamberSign France se réserve le droit de révoquer le Certificat conformément au chapitre « Révocation du certificat » des présentes CGU.

102. Le Client et son Représentant Légal sont garants de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.

103. Le Client et son Représentant Légal reconnaissent et acceptent que les informations fournies à ce titre soient conservées et utilisées par ChamberSign France pour gérer les Certificats dans les conditions prévues par la loi en vigueur et en particulier celles relatives à la protection des données à caractère personnel.

104. Le Client et son Représentant Légal reconnaissent être informés des conditions d'installation des Certificats de ChamberSign France. En particulier, le Certificat fait l'objet d'un tutoriel disponible sur le site Internet de ChamberSign France.

105. Le Client et son Représentant Légal choisissent le matériel et les logiciels offrant une sécurité en adéquation avec leurs besoins pour l'installation et la protection des Certificats et des supports physiques.

## 12. Obligations du Porteur de certificat

106. Le Porteur de certificat est tenu de vérifier la validité du certificat et la conformité de son utilisation.

107. Le Porteur s'engage à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des Certificats pendant toute la durée du contrat.

108. Le Porteur est garant de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.



109. Le Porteur reconnaît et accepte que les informations fournies à ce titre soient conservées et utilisées par ChamberSign France pour gérer les Certificats dans les conditions prévues par la loi en vigueur et en particulier celles relatives à la protection des données à caractère personnel.

110. Le Porteur informe immédiatement ChamberSign France de toute modification concernant les informations contenues dans son Certificat, laquelle entraînera une révocation de son certificat conformément à l'article « Révocation du Certificat » des présentes CGU. A défaut d'information préalable délivrée par le Porteur à ChamberSign France, la responsabilité de ChamberSign France ne pourra pas être engagée au titre d'une information non conforme à la réalité.

111. ChamberSign France se réserve la faculté de procéder à des vérifications aléatoires concernant l'actualité des informations contenues dans le Certificat.

112. Le Porteur de certificat s'engage à informer le BE de rattachement de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, sans délais. A défaut de se faire, le Client devra s'en charger, conformément à l'article précédent.

113. Le Porteur de certificat reconnaît être informé des conditions d'installation des Certificats et du tutoriel disponible sur le site Internet de ChamberSign France.

114. Le Porteur de certificat s'engage à respecter les usages autorisés des Bi-clés et des Certificats.

115. Le Porteur de certificat protège sa Clé Privée par des moyens appropriés à son environnement. Il s'engage notamment à ne pas communiquer à un tiers son code PIN ou les réponses à ses questions de sécurité.

116. Le Porteur de certificat protège ses données d'activation et, le cas échéant, les met en œuvre.

117. Le Porteur de certificat respecte les conditions d'utilisation de sa Clé Privée et du Certificat correspondant.

118. Le Porteur de certificat doit faire, sans délai, une demande de révocation de son Certificat en cas de Compromission ou de suspicion de Compromission de sa Clé Privée (ou de ses données d'activations).

119. Le Porteur de certificat s'engage à ne pas prêter ou confier le Certificat qui lui est attribué ni les codes de protection de ce Certificat à une quelconque tierce personne.

120. Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation.

### **13. Obligations des Utilisateurs de certificats**

121. Les Utilisateurs de Certificats sont informés de la nature et de la qualification du Certificat tel qu'indiqué à l'article « Définitions » des présentes CGU, en particulier que celui-ci ne peut être utilisé que pour des services d'Authentification et de Signature électronique.

122. Les Utilisateurs de Certificats vérifient et respectent l'usage pour lequel un Certificat a été émis.





123. Les Utilisateurs de Certificats contrôlent que le Certificat émis par ChamberSign France est référencé au niveau de sécurité et pour le service de confiance requis par l'application.

124. Lorsque le Porteur n'est pas le Représentant Légal de l'Entité, l'Utilisateur du Certificat vérifie que le Porteur dispose, à la date de signature, des pouvoirs nécessaires pour engager l'Entité pour l'acte concerné.

125. Pour chacun des Certificats de la chaîne de Certification, du Certificat du Porteur jusqu'à l'Autorité de Certification racine, les Utilisateurs du Certificat vérifient l'état du Certificat et notamment la signature numérique de ChamberSign France, émettrice du Certificat considéré, et contrôlent la validité de ce Certificat.

126. Les Utilisateurs de Certificats vérifient et respectent les obligations des Utilisateurs de Certificats exprimés dans la PC concernée applicable.

## **14. Prix et facturation**

### **14.1. Prix**

127. Le prix des Certificats est déterminé dans les conditions tarifaires émises par ChamberSign France.

128. Les modes de règlement acceptés sont les suivants :

- Carte bancaire ;
- Virement ;
- Mandat ;
- Chèque.

129. Aucun escompte n'est accordé en cas de règlement anticipé.

130. ChamberSign France facturera au Client les frais bancaires dans le cas où le chèque serait émis sans provision, ainsi que les frais engendrés en cas d'erreur de paiement de la part du Client ou en cas de double paiement.

131. Le prix est exigible dès réception de la facture, qui est émise immédiatement après le téléchargement du Certificat.

132. Par exception à ce qui précède, le Client peut demander, lors de sa demande de Certificat, à bénéficier d'un paiement échelonné annuellement et ce sur une période de trois (3) ans (durée de vie d'un certificat). Dans ce cas, la première facture est émise à la date de génération du certificat, les factures suivantes à la date d'anniversaire du téléchargement et exigible dès leur émission, à moins que le Client ou le Porteur n'ait révoqué le certificat avant sa date d'anniversaire.

133. Les paiements sont exigibles à leur échéance même si les factures émises par ChamberSign France ne mentionnent pas les numéros de commande ou toute autre mention spécifique au Client.

134. Le Client reconnaît expressément que le prix du service est dû en totalité pour la période facturée nonobstant la révocation du Certificat avant son terme, quelle que soit la cause de la révocation. En cas de paiement échelonné, seule la période annuelle en cours de



facturation est due. Le Client pourra donc être tenu par voie de justice ou par l'intervention d'un officier ministériel (huissier) de régler le solde des sommes dues.

135. En cas de non-règlement dans les délais, il sera dû conformément à l'article L 441-6 du Code de Commerce, une indemnité calculée sur la base du taux d'intérêt appliqué par la banque centrale européenne à son opération de refinancement la plus récente majoré de 10 points de pourcentage, ainsi qu'une indemnité forfaitaire pour frais de recouvrement d'un montant de quarante (40) €. Par exception à ce qui précède, la majoration susvisée sera de 8 points de pourcentage en cas de commande publique.

136. Ces pénalités seront applicables dès le jour suivant la date prévue au règlement de la facture et seront exigibles sans qu'aucun rappel ne soit nécessaire.

137. En cas de non-règlement, le Certificat sera révoqué de plein droit sans ouvrir droit à dommages et intérêts ni remplacements.

## **14.2. Facturation**

138. Les factures originales sont émises par ChamberSign France sous format électronique et sont adressées par email au Porteur ou à toute autre adresse email indiquée à cet effet par le Porteur lors de la demande de Certificat. Le Porteur et le Client s'engagent à notifier tout changement d'adresse email à ChamberSign France.

139. Il ne sera fait droit à aucune demande d'envoi de facture papier.

140. Une facture est établie par Certificat, même si le Client dispose de plusieurs Certificats. L'établissement d'une facture globale ou la modification de facture à la demande du Client donnera lieu à un surcoût fixe de quarante (40) Euros HT en ajoutant cinq (5) Euros HT par certificat (frais d'annulation de chaque facture).

141. La dénomination sociale et l'adresse du Client indiquées lors de la demande de Certificat seront celles utilisées pour l'édition des factures. Aucune modification de ces données ne pourra être apportée aux factures comme au Certificat. En cas de modification des informations contenues dans le Certificat, le Certificat devra être révoqué et une nouvelle demande de Certificat devra être faite, selon les modalités définies par les CGU.

## **15. Responsabilité**

142. ChamberSign France est responsable de la conformité de sa Politique de Certification, avec les exigences émises par la PC-Type.

143. ChamberSign France assume toute conséquence dommageable résultant du non-respect de sa Politique de Certification par elle-même ou l'une de ses composantes.

144. ChamberSign France reconnaît engager sa responsabilité en cas de faute ou de négligence prouvées, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats.

145. ChamberSign France est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.



146. ChamberSign France ne saurait être tenue responsable du préjudice causé par un usage du Certificat dépassant les limites de l'usage autorisé.

147. La responsabilité de ChamberSign France ne saurait être engagée en cas d'informations inexactes dues à de fausses déclarations, à de faux documents ou à l'absence d'information des modifications survenues dans la situation du Client, du Porteur, du Représentant Légal, ou du Mandataire de Certification lors de la création ou en cours de validité du Certificat, que la fausse déclaration, le faux document ou l'omission soit intentionnel ou pas.

148. ChamberSign France n'assume aucun engagement, ni aucune responsabilité quant aux conséquences des retards de transmission, altération, erreurs ou pertes de tout message électronique, lettre ou document signés ou authentifiés.

149. ChamberSign France ne saurait en aucun cas être tenue responsable du contenu des fichiers ou transactions signés ou authentifiés en utilisant le Certificat, le Client et le Porteur étant seuls responsables vis-à-vis des tiers du contenu de ces envois.

150. Sans préjudice de l'article « Assurance » des présentes CGU, ChamberSign France ne sera en aucun cas tenue responsable des dommages indirects tels que, par exemple, tout préjudice financier ou commercial, perte de bénéfice ou d'exploitation, trouvant leur origine ou étant la conséquence de l'abonnement ou inhérents à l'utilisation des Certificats émis par ChamberSign France.

151. ChamberSign France n'assume aucun engagement ni responsabilité quant à l'utilisation par le Porteur d'un Certificat non conforme aux dispositions des CGU, notamment pour ce qui concerne les procédures de contrôle de validité du Certificat lors d'une transaction.

152. Par ailleurs, ChamberSign France ne saurait être responsable des phénomènes liés à l'usure normale des médias informatiques, et notamment de la détérioration des informations portées sur lesdits médias due à l'influence des champs magnétiques.

153. ChamberSign France ne saurait être tenue pour responsable des dommages liés notamment à une interruption ou un dysfonctionnement des services et applications de l'Utilisateur de Certificats.

154. Si le Représentant Légal a fait l'acquisition d'un ou plusieurs supports physiques, ChamberSign France n'est responsable que de leur délivrance physique.

155. Du fait de l'évolution constante de la technologie et des niveaux de sécurité attachés au référentiel en vigueur, en cas de dysfonctionnement du support physique ou de son logiciel pilote associé, le Client devra demander la révocation du Certificat.

156. ChamberSign France ne saurait être responsable de l'usage de la Clé Privée du Porteur, qui en a la responsabilité personnelle. Tout dommage lié à la Compromission de la Clé Privée est à la charge du Client.

157. ChamberSign France ne saurait voir sa responsabilité engagée du fait d'une utilisation illicite du Certificat dès lors que le Client, le Représentant Légal, le Mandataire de Certification ou le Porteur n'aura pas effectué une demande de révocation conformément aux CGU.

## **16. Sécurité**

158. Chambersign France fait ses meilleurs efforts, conformément aux règles de l'art, pour sécuriser les systèmes d'information qu'elle utilise contre les risques d'intrusion non-autorisée



ou manipulation de ses données et s'engage à mettre en œuvre toutes les mesures utiles pour préserver l'intégrité des Certificats et des Bi-Clés.

159. Chambersign France s'engage à mettre à jour l'analyse de risques sur le système d'information utilisé pour mettre en œuvre ses services à chaque modification ayant un impact important sur le service qu'elle fournit, notamment en cas de modification de la Politique de Certification ou pratiques relatives à la fourniture du service.

160. Chambersign France s'engage à informer l'Agence Nationale de la Sécurité des Systèmes d'Information de tout changement ou cessation de ses activités concernant la délivrance de certificats qualifiés.

161. Chambersign France s'engage à notifier à l'Agence Nationale de la Sécurité des Systèmes d'Information ainsi qu'à la Commission Nationale de l'Informatique et des Libertés toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui sont conservées.

162. Lorsque l'atteinte à la sécurité ou la perte d'intégrité est susceptible de porter préjudice à une personne physique ou morale à laquelle le service de certification a été fourni, Chambersign France s'engage à notifier, dans les meilleurs délais, à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité.

## **17. Assurance**

163. ChamberSign France a souscrit, pour l'ensemble des dommages corporels, matériels et immatériels résultant de son activité une assurance couvrant les conséquences de sa responsabilité civile professionnelle.

164. Aux termes du contrat d'assurance souscrit par ChamberSign France, et dans les limites et conditions de ce contrat, le Porteur pourra bénéficier du remplacement du Certificat perdu, ou volé.

## **18. Confidentialité**

165. Toutes informations ou toutes données communiquées par les parties, par écrit ou oralement, relativement aux Certificats sont considérées comme confidentielles.

166. Les parties s'engagent à :

- traiter les informations confidentielles avec le même degré de protection qu'elles accordent à leurs propres informations confidentielles de même importance ;
- garder les informations confidentielles et qu'elles ne soient pas divulguées ni susceptibles de l'être directement ou indirectement à tout tiers ;
- éviter que les informations confidentielles ne soient ni copiées, ni reproduites, ni dupliquées, en partie ou en totalité, lorsque de telles copies, reproductions ou duplications ne sont pas directement liées à l'exécution des présentes.

## 19. Propriété intellectuelle

167. Les parties déclarent et garantissent avoir la libre disposition des marques, noms, dénominations, et autres signes distinctifs destinés à être utilisés dans le cadre des présentes.

168. A l'exception de l'utilisation des Certificats prévue par les CGU, le Client et le Porteur ne pourront faire état ou usage des marques, des dessins, des modèles, des images, des textes, des photos, des logos, des chartes graphiques, des logiciels, des moteurs de recherche, des bases de données, des documents, sans que cette liste ne soit exhaustive ou tout autre droit de propriété intellectuelle appartenant à ChamberSign France qu'avec l'autorisation expresse, écrite et préalable de celle-ci.

169. Les CGU n'emportent aucune cession d'aucune sorte de droits de propriété intellectuelle sur tout ou partie des éléments appartenant à Chambersign France ou à ses partenaires et tiers qui lui ont concédé une licence.

170. Toute reproduction ou représentation, totale ou partielle d'un de ces éléments, sans l'autorisation expresse de Chambersign France est interdite et constituerait une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

171. En conséquence, le Client et le Porteur s'interdisent tout agissement et tout acte susceptible de porter atteinte directement ou indirectement aux droits de propriété de Chambersign France.

## 20. Traitement des données à caractère personnel

172. Voir Annexe 1.

## 21. Résiliation de l'abonnement

173. Dans le cas d'une souscription à l'abonnement « Offre Sérénité trois (3) ans » de ChamberSign France, le Client pourra résilier l'abonnement à tout moment et sans cause. En revanche, la période annuelle en cours de facturation sera due.

174. Dans le cas où le Client opte pour un abonnement « Offre annuelle avec tacite reconduction » de ChamberSign France via un paiement échelonné annuellement pendant la durée de validité du Certificat, toute année entamée sera due. La résiliation sera prise en compte pour le paiement de l'abonnement de ou des année(s) suivante(s).

175. Dans ce cas, l'abonnement « Offre annuelle avec tacite reconduction » sera considéré résilié à compter de l'envoi par le Client d'une lettre recommandée avec accusé de réception ou d'un mail signé électroniquement à chaque période annuelle moyennant un préavis de trois (mois) avant la date d'anniversaire du ou des Certificat(s) à l'adresse suivante : ChamberSign France, 10, Cours de Verdun Rambaud – 69002 Lyon ou à [facturation@chambersign.fr](mailto:facturation@chambersign.fr). La résiliation susvisée interviendrait sans préjudice de tous dommages et intérêts que serait en droit d'obtenir ChamberSign France.

176. Le Client ne pourra prétendre au remboursement des sommes déjà versées au titre de l'abonnement aux services de certification délivrés par ChamberSign France.

177. De son côté, par dérogation expresse à l'article 1225 du Code civil et sans préjudice de tous dommages et intérêts auxquels elle pourrait prétendre, ChamberSign France pourra résilier l'abonnement de façon anticipée en cas de manquement par le Client ou le Porteur aux



obligations contractuelles mises à leur charge, notamment aux obligations relatives au paiement du prix ou celles concernant l'utilisation du Certificat conforme aux CGU, après envoi d'une lettre recommandée avec accusé de réception (postal ou électronique) notifiant le manquement en cause et visant la présente clause restée infructueuse pendant 30 jours.

178. La résiliation constitue une cause de révocation des Certificats.

179. Si après révocation, ChamberSign France reçoit de la même personne une nouvelle demande de Certificat, un nouveau dossier sera constitué et les CGU seront alors de nouveau à signer.

180. Dans le cas d'une résiliation intervenant avant la fin de la durée de validité attachée au Certificat, pour un motif non imputable à ChamberSign France, le prix versé par le Client restera acquis à ChamberSign France, et ce quel que soit le type d'abonnement choisi.

## 22. Conservation

181. Le Client consent à ce que ChamberSign France conserve les documents relatifs à la preuve du contrôle d'identification des Porteurs pendant les délais prévus dans la Politique de Certification ainsi que les documents relatifs à la conclusion du présent contrat.

182. Les journaux d'évènements sont conservés sur site pendant une durée de trente (30) jours. Après leur génération, ils sont archivés et conservés pendant sept (7) ans.

183. Il appartient au client de conserver une copie du présent Contrat préalablement imprimé par ses soins, de le signer de manière manuscrite et de retourner l'entier dossier au Bureau d'Enregistrement. Les dossiers d'enregistrement sont archivés pendant une durée de onze (11) ans à compter de la délivrance du Certificat. Les dossiers (en version papier et électronique) sont archivés chez des tiers archiveur, sur des sites sécurisés et dont les données sont accessibles qu'aux personnes autorisées. Toute demande de duplicata du dossier d'enregistrement à ChamberSign France sera facturée cinquante (50) Euros HT au Client.

184. Les Certificats et les LCR sont archivés pendant une durée de cinq (5) ans après leur expiration.

185. Si le Client souhaite que les dossiers d'enregistrement, les Certificats ou les LCR soient conservés pour une durée d'archivage supérieure, il devra en faire le nécessaire et en prendre le coût lui-même à sa charge.

186. Les clés privées des Porteurs ne font l'objet d'aucun séquestre et d'aucune sauvegarde.

## 23. Nullité

187. Si une ou plusieurs clauses des CGU sont tenues pour non valables ou déclarées comme telles par une loi, un règlement ou par suite d'une décision définitive d'une juridiction compétente, les autres clauses conserveront leur pleine validité sauf en cas de caractère indissociable avec la stipulation litigieuse.

## **24. Intégralité**

188. Les parties reconnaissent que les CGU, le formulaire d'abonnement, le tarif applicable et la Politique de Certification de ChamberSign France concernée ainsi que tout document contractuel relatif à la délivrance et à la gestion des Certificats constituent l'intégralité du contrat.

189. En cas de contradiction, les dispositions des présentes prévaudront sur tout autre document des parties et notamment sur les conditions générales d'achat du Client.

## **25. Règlement des litiges – tribunal compétent – loi applicable**

190. En cas de difficulté de toute nature et avant toute procédure juridictionnelle, les parties s'engagent à mettre en œuvre une procédure de conciliation.

191. Les parties s'engagent à se réunir à l'initiative de la partie la plus diligente dans les huit jours à compter de la réception de la lettre de demande de réunion de conciliation.

192. L'ordre du jour est fixé par la partie qui prend l'initiative de la conciliation.

193. Les décisions, si elles sont arrêtées d'un commun accord, ont valeur contractuelle.

194. Cette clause est juridiquement autonome du présent contrat. Elle continue à s'appliquer malgré l'éventuelle nullité, résolution, résiliation ou anéantissement des présentes relations contractuelles.

195. A défaut, compétence expresse est attribuée aux tribunaux français.

196. Les présentes CGU sont régies par la loi française.

197. Il en est ainsi pour les règles de fond et les règles de forme et ce, nonobstant les lieux d'exécution des obligations substantielles ou accessoires.

## **26. Lien de publication de la Politique de Certification et des documents d'engagements**

198. La Politique de certification concernée applicable est publiée à l'adresse suivante : [https://pc.chambersign.fr/ca3/ChamberSign\\_France\\_CA3\\_Qualified\\_eID.pdf](https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf)

## **27. Espace de publication et conformité**

199. Les certificats émis sont qualifiés eIDAS.

200. Le certificat racine de l'IGC est téléchargeable sur le site Web de ChamberSign.

201. L'utilisateur peut vérifier l'empreinte du certificat racine sur le site sécurisé <https://www.keymanagement.chambersign.fr> ou en contactant ChamberSign France par téléphone.



202. Les points de publication des LCR sont les suivants :  
[http://crl.chambersign.fr/ca3/ChamberSign\\_France\\_CA3\\_Qualified\\_eID.crl](http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl) et  
[http://crl.chambersign.tm.fr/ca3/ChamberSign\\_France\\_CA3\\_Qualified\\_eID.crl](http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl)
203. Le certificat d'AC est téléchargeable à l'adresse  
[https://pc.chambersign.fr/ca3/ChamberSign\\_France\\_CA3\\_Qualified\\_eID.cer](https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.cer)
204. Les répondeurs OCSP sont accessibles aux adresses suivantes :  
[http://ocsp\\_ca3.chambersign.fr/ChamberSign\\_France\\_CA3\\_Qualified\\_eID](http://ocsp_ca3.chambersign.fr/ChamberSign_France_CA3_Qualified_eID) et  
[http://ocsp\\_ca3.chambersign.tm.fr/ChamberSign\\_France\\_CA3\\_Qualified\\_eID](http://ocsp_ca3.chambersign.tm.fr/ChamberSign_France_CA3_Qualified_eID)
205. Les profils de certificats, de LCR sont conformes à la norme ETSI 319412.
206. Les certificats produits contiennent les extensions qualifiées suivantes : id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, i-etsi-qct-esign, QcEuPDS.



## ***ANNEXE 1. PROTECTION DES DONNEES A CARACTERE PERSONNEL***

### **1. Données à caractère personnel**

#### ***1.1 Traitement de données à caractère personnel***

1. Pour ChamberSign France, la protection des données personnelles est fondamentale car elle reflète les relations que nous entretenons avec vous. Il nous tient à cœur de protéger votre vie privée et celle de vos partenaires et collaborateurs, au regard des informations que vous nous confiez.

2. Le présent article a pour objectif principal de vous informer sur la collecte et l'utilisation de vos données personnelles par notre Association, dans le cadre de la fourniture de nos services. Les données collectées par Chambersign sont donc strictement nécessaires à la réalisation de nos prestations.

3. Conformément au Règlement européen n°2016/679 dit règlement général sur la protection des données (RGPD) et aux dispositions de la loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, ChamberSign agit en tant que Responsable de traitement concernant la collecte et le traitement des données à caractère personnel des utilisateurs de ses services. Nous sommes donc responsables du respect des obligations issues de ce texte.

4. Les présentes stipulations ne concernent pas les traitements de données personnelles que ChamberSign peut être amenée à opérer en qualité de sous-traitant.

5. A ce titre, les données à caractère personnel recueillies par ChamberSign France pour les besoins de la délivrance et de la conservation des Certificats sont des données d'identité (nom, prénom), ainsi que des données relatives à votre vie professionnelle (fonction, service, email professionnel). ChamberSign France ne collecte aucune donnée sensible comme la religion, l'appartenance syndicale, les origines raciales et ethniques, les condamnations pénales ou les données relatives à la santé.

6. ChamberSign France recueille les données personnelles de ses clients et les traite pour des finalités inhérentes à la fourniture de ses services de certification. Le traitement de vos données personnelles repose donc sur le respect de nos obligations contractuelles. Dans ce cadre, nous collectons vos données personnelles afin de vous fournir nos services de certification, de gérer et de suivre le cycle de vie de vos certificats et Bi-clés (délivrance, conservation, renouvellement, révocation) ou encore de suivre notre relation commerciale.

- La fourniture des services de certification par ChamberSign France ;
- La gestion de l'accès et du fonctionnement des services de certification fournis par ChamberSign France ;
- L'identification du Porteur ou du Responsable de Certificat ;
- L'authentification du Porteur ou du Responsable de Certificat ;



- La délivrance, la conservation, le renouvellement et la révocation des Certificats et des Bi-clés ;
- L'établissement de statistiques et la mesure de la qualité et de la satisfaction des services de certification fournis par ChamberSign France ;
- Le suivi de la relation commerciale : vos données pourront être utilisées afin de communiquer sur les actualités de ChamberSign France et notamment sur le renouvellement des produits et les nouveautés proposées, jusqu'à trois (3) ans à compter de la fin de notre relation commerciale.

7. Les informations collectées sont obligatoires. A défaut, Chambersign France ne pourra pas fournir les services de certification.

8. Les données collectées sont seulement destinées aux services habilités de ChamberSign France. Une partie de ces données pourra être transmise aux sous-traitants de ChamberSign France, qui respectent la même politique de confidentialité que ChamberSign France. Les données transmises seront strictement limitées aux besoins définis pour l'exécution de la mission du sous-traitant.

9. ChamberSign France ne procède et ne procédera à aucune vente de vos données personnelles. Les données traitées par ChamberSign France ne font pas non plus l'objet d'un transfert en dehors de l'Union européenne.

10. En application du Référentiel Général de Sécurité (RGS Annexe A2, Politique de Certification Type « Certificats électroniques de personne », version 3 du 27 février 2014) et des présentes CGU, nous conservons vos données onze (11) ans à compter de la délivrance du certificat.

11. Conformément à la Règlementation en vigueur, vous disposez d'un droit d'accès, de rectification, d'effacement, de limitation du traitement et d'opposition.

12. Afin d'exercer vos droits, vous pouvez nous contacter par courrier accompagné d'une copie d'une pièce d'identité signée à l'adresse suivante : ChamberSign France – 10, Cours de Verdun Rambaud – 69002 LYON ou bien par courrier électronique à l'adresse suivante : [rgpd@chambersign.fr](mailto:rgpd@chambersign.fr), étant précisé que pour sécuriser l'authentification, l'envoi d'un mail signé électroniquement est privilégié ; l'envoi d'une pièce d'identité scannée (carte d'identité, passeport...) est prohibé afin de garantir la confidentialité des données. En l'absence de signature électronique, ChamberSign France procédera à l'authentification du demandeur par tout moyen approprié, ceci pour éviter toute divulgation des données à caractère personnel.

13. Pour en savoir plus sur l'utilisation de vos données et sur l'exercice de vos droits issus de la Loi Informatique et Libertés ainsi que du RGPD, vous pouvez consulter notre [politique de protection des données](#) ou contacter notre Délégué à la Protection des données.

14. Par ailleurs, nous vous informons que vous détenez le droit d'introduire une réclamation devant une autorité de contrôle (CNIL) : <https://www.cnil.fr/fr/agir>.

## 2. Cookies

15. Lorsque l'Utilisateur visite notre site Internet, des cookies sont envoyés à son ordinateur, sa tablette ou son téléphone mobile. Afin de mieux protéger l'Utilisateur face aux cookies tout en comprenant leur utilité, ChamberSign a adopté une [Politique d'utilisation des cookies](#) qui fait partie intégrante des présentes Conditions, consultable depuis notre Site et que l'Utilisateur est expressément invité à consulter.