



1. PREAMBULE

1. ChamberSign France est une société par actions simplifiée au capital de 496 000 euros, dont le siège est sis 8-10 Rue Pierre Brossolette 92300 Levallois-Perret, et dont l'établissement principal ainsi que l'adresse de correspondance sont situés Le Cours du Midi, 10, Cours de Verdun Rambaud 69002 Lyon, immatriculée au Registre du Commerce et des Sociétés de Nanterre sous le numéro 433 702 479.

2. ChamberSign France met à la disposition du Client et de son Représentant Légal, du RCC 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 RCC, et l'utilisateur du Certificat reconnaissent avoir lu, compris et approuvé les CGU ainsi que la PC du Certificat dont l'OID est 1.2.250.1.96.1.8.2.5, acceptent pleinement leur contenu et reconnaissent être liés par la totalité de leurs dispositions.

5. Le Client, son Représentant Légal, le RCC 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 RCC, 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. DEFINITIONS

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 de site WEB ;

- « 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 CA3 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 RCC 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 RCC et à la vérification et validation du dossier 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 titulaire de certificat ;
- l'adresse du/des sites web à protéger ;
- optionnellement des codes d'identification du titulaire
- la clé publique du RCC de certificat ;
- le/les 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 détenteur 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 RCC 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 et au RCC ;

- « 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 perte éventuelle 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 ;

- « Demandeur » : désigne toute personne physique qui initialise une demande de certificat, sans pouvoir d'engagement ni pour le titulaire, ni pour l'entité à laquelle le certificat est rattaché, excepté s'il s'agit du titulaire lui-même, du représentant légal de l'entité, de son déléataire le cas échéant, ou bien d'une tierce personne. Le demandeur est donc une personne chargée de saisir les informations qui seront validées par les acteurs concernés par la demande ;

- « Données Confidentielles » : désigne 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 RCC qui devront être impérativement gardées secrètes ;

- « 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, 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 ;
- « OID » : désigne le numéro d'identifiant objet désignant la Politique de Certification de l'Autorité de Certification ou une référence de certificat ;
- « Politique de Certification » ou « PC » : désigne l'ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une AC déclare se conformer dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'application avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats ;
- « Règlement eIDAS » : Règlement (UE) du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, modifié par le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024. Il impose notamment des exigences relatives à la reconnaissance mutuelle des moyens d'identification électronique ainsi qu'à celle des signatures électroniques.
- « Représentant Légal » : désigne le Représentant Légal du Client ;
- « Responsable de Certificat » ou « RCC » : désigne la personne en charge et responsable du certificat électronique de type cachet ou d'authentification serveur ;
- « Révocation du Certificat » : action demandée par une entité autorisée (AC, MC, RCC, etc.) et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la perte de la carte, la compromission d'une clé, le changement d'informations contenues dans un certificat, etc. ;
- « RGPD » : signifie 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 ;
- « 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 ;
- « 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.
- « Titulaire » : désigne soit le porteur pour une personne physique, soit une personne morale, représentée par le RCC, au nom duquel un certificat a été délivré.
- « Utilisateur du Certificat » : désigne l'entité ou la personne physique qui se connecte à un site Internet ou une ressource serveur sous protocoles SSL/TLS et qui fait confiance à l'identité protégée par le Certificat QWAC (QNCP-w-gen).
- « QWAC » : désigne un certificat qualifié d'authentification de site web délivré à une personne morale par un prestataire de services de confiance qualifié conformément au règlement eIDAS.

3. OBJET

8. Les CGU ont pour objet de définir les conditions selon lesquelles le Client pourra utiliser les Certificats tels que définis à l'article 2 Définitions et émis par ChamberSign France en tant qu'Autorité de Certification, conformément à sa Politique de Certification.

4. CONTACT

9. Toute demande peut être adressée à :

- Chambersign France : Immeuble Le Cours du Midi, 10 cours de Verdun Rambaud – 69002 LYON
- qualite@chambersign.fr

5. DUREE – ENTREE EN VIGUEUR – OPPOSABILITE

10. Les CGU sont opposables au Client et au RCC 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.

11. Les CGU sont conclues et opposables pendant toute la durée de vie du Certificat, d'une période maximale de un an, 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.).

12. 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.

13. 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 RENOUELEMENT

6.1 Enregistrement des dossiers de demande de certificat

14. Le RCC, et le Représentant Légal du Client peuvent faire une demande de Certificat en se connectant sur le site Internet de ChamberSign France : www.chambersign.fr. La création d'un Espace Client sera requise pour finaliser la commande du Client (se reporter aux CGU de l'Espace Client lors de votre inscription).

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

16. Le Client doit envoyer les pièces justificatives nécessaires au BE (sous format papier, dématérialisé ou en main propre).

6.2 Vérification de la demande

17. Le BE, composé d'opérateurs de confiance habilités à vérifier les demandes de certificats, réalise les opérations suivantes :

- vérifie et valide l'identité du futur RCC au niveau substantiel dont l'adresse mail doit être nominative ;
- vérifie la cohérence des justificatifs présentés ;
- s'assure que le futur RCC dispose bien de l'autorisation de la part du Représentant légal à faire une demande de certificat pour le certificat QWAC ;
- s'assure que le futur RCC a pris connaissance des CGU, des modalités applicables pour l'utilisation du Certificat et a accepté les CGU.

18. L'identité du responsable de certificat est vérifiée au moyen de documents dont une copie certifiée conforme par le RCC est transmise par courrier ou en électronique.

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

20. Les informations concernant la structure à laquelle le RCC est rattaché ainsi que la propriété des noms de domaines du certificat font l'objet de vérification lors de l'enregistrement (existence, validité...).

6.3 Rejet de la demande

21. En cas de pièces manquantes, le Client reçoit une notification sur son Espace Client afin de régulariser sa demande. En cas de non-régularisation de sa part et après relance quant à la communication de ces pièces, le BE se réserve le droit de rejeter la demande de Certificat.

22. Le BE en informe le RCC, ou le Représentant Légal du Client.

6.4 Délivrance du certificat

23. Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC ainsi que l'obtention d'un code de retrait, le processus consiste à remettre au responsable de certificats la clé publique certifiée par l'AC : génération de la bi-clé, sous le contrôle et la responsabilité du RCC, dans un support cryptographique (logiciel ou matériel) choisi par le RCC (moyennant le respect des exigences définies au chapitre 6.2 ci-dessus), envoi de la clé publique à la fonction de génération des certificats, téléchargement sur le support du certificat généré.

24. Les certificats sont émis conformément au profil défini dans le document [GUI.ACC.11] en cliquant [ici](#).



25. Après authentification de l'origine et vérification de l'intégrité de la demande provenant du BE, ChamberSign France génère le Certificat et les données de révocation, ce que le RCC accepte.

26. 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 RCC qui devra suivre les indications décrites pour en effectuer le retrait.

27. Chaque Responsable de Certificat peut choisir librement son support cryptographique.

28. Les clés privées des Certificats ne font l'objet d'aucun séquestre et d'aucune sauvegarde par ChamberSign France.

29. Le RCC s'engage à mettre en œuvre le certificat délivré dans un environnement garantissant que le RCC garde le contrôle sur la clé privée correspondante.

30. Le retrait des Certificats s'effectue dans les deux mois suivant la réception du message informant le RCC de la mise à disposition du Certificat.

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

6.5 Acceptation du certificat

32. Le certificat fait l'objet d'une acceptation implicite par le responsable de certificats suite à son téléchargement.

33. Toute demande de modification du Certificat nécessite pour le RCC d'effectuer une nouvelle demande de Certificat.

6.6 Assistance

34. Afin d'accompagner le RCC, 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 et horaires accessibles sur le lien suivant : <https://www.chambersign.fr/p-nous-contacter/>)

35. Des guides ainsi qu'une foire aux questions sont disponibles sur le site Internet de ChamberSign France à l'adresse suivante : <https://support.chambersign.fr/guides/>

6.7 Renouvellement

36. 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 QWAC est au maximum de un (1) an. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque cryptographique.

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

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

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

40. 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 RCC 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 du Certificat sur le site Internet de ChamberSign France, depuis son Espace Client.

41. 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.

6.8 Modification du certificat

42. 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.

43. 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

44. Le mot de passe nécessaire à l'utilisation du Certificat par le RCC n'est enregistré sur aucune base et n'est connu que du RCC. En conséquence, en cas de perte du mot de passe, ChamberSign ne sera pas en mesure de le récupérer et le Certificat devra être révoqué. Une nouvelle demande de Certificat devra alors être faite, selon les modalités définies par les CGU.

7. CONDITIONS D'USAGE DES CERTIFICATS ET LIMITES

45. L'usage est l'authentification d'un serveur sur la base de son nom de domaine. Le certificat d'authentification serveur permet à toute application utilisatrice de s'assurer de l'identité de l'entité légale et du nom de domaine pour lesquels le certificat a été émis. Il garantit également l'intégrité des données qui sont échangées entre l'application utilisatrice et le serveur.

46. L'utilisation de la Clé Privée du RCC et du Certificat doit rester strictement limitée aux services d'Authentification.

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

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

49. 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.

8. PROCEDURE DE VERIFICATION DES CERTIFICATS

50. ChamberSign France s'engage à mettre à disposition, 24h/24, un service de consultation sur son site internet <https://support.chambersign.fr/lcr/> permettant de vérifier la validité des Certificats qu'elle a émis.

51. 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.

52. 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.

53. Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat objet des présentes PC :

- la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du responsable de certificat lui-même) ;
- les informations 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 responsable du certificat 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 responsable du certificat a changé et n'a pas été remplacé

54. Les causes de révocation ne sont jamais publiées.



9. REVOCATION DU CERTIFICAT

55. 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 ;
- compromission possible ou avérée de la Clé Privée du RCC ;
- dysfonctionnement du support physique ou de son logiciel pilote associé ;
- non-respect par le RCC des règles d'utilisation du Certificat ou des présentes CGU ;
- non-respect par le RCC ou le Client de la PC de ChamberSign France CA3 NG Qualified eID ;
- réalisation d'opérations frauduleuses ;
- résiliation de l'abonnement ;
- demande de révocation du Certificat par le Client ;
- demande de révocation du Certificat par le RCC ;
- cessation de l'activité du RCC au sein du Client et ce, quelle qu'en soit la cause : décès, démission... ;
- vol ou perte du support physique du Certificat ou perte du mot de passe pour un certificat logiciel ;
- cessation d'activité du Client.

56. 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 main propre au BE, ou en ligne à partir du site Internet suivant: <https://support.chambersign.fr/revocation-certificat-electronique/> ou par le Représentant Légal via son Espace Entreprise dont les accès lui ont été communiqués par mail.

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

- le Représentant Légal du Client ;
- le Responsable de Certificat ;
- ChamberSign France.

58. En cas de vol ou de perte du mot de passe du Certificat, la demande de révocation du RCC devra porter sur son Certificat dans les plus brefs délais.

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

60. 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.

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

62. Le RCC 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 RCC.

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

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

65. 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.

66. La fonction de gestion des révocations est disponible 24 heures sur

24, 7 jours sur 7.

67. Les demandes de révocation sont traitées dans les 24h suivant la réception de la demande, 7 jours / 7 (week-ends et jours fériés compris si la révocation est faite en ligne), hors révocations consécutives à des demandes de modification des données du RCC.

68. La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2h (jours ouvrés).

69. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 16h (jours ouvrés).

10. OBLIGATIONS DE CHAMBERSIGN

70. 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 de sa PC.

71. Elle s'engage au contrôle par le BE de l'identification du RCC et du Représentant Légal, se présentant pour obtenir un Certificat.

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

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

74. Elle s'engage à tout mettre en œuvre pour créer et émettre des Certificats contenant des informations réputées exactes.

75. 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.

76. Elle s'engage à ce que le Certificat soit prêt à la délivrance pour le RCC dans un délai de 48 heures à compter de la remise d'un dossier complet au BE, excepté lors de périodes de ralentissement de l'activité (fêtes, période estivale ou encore effectif réduit) où les délais peuvent être allongés dans la limite d'une durée raisonnable.

77. Elle 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.

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

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

80. ChamberSign France prend toutes les mesures raisonnables pour s'assurer que les RCC 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.

81. 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.

82. 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.

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

11. OBLIGATIONS DU CLIENT

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

85. Le Client et son Représentant Légal sont responsables de la gestion des Certificats délivrés aux employés, délégataires ou agents du Client dans le cadre du contrat d'abonnement et s'engage à faire en sorte que tout Responsable 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 RCC :

- 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 9 Révocation du Certificat ;
- conserve secrètes, de manière sécurisée et sous son contrôle, les données confidentielles du Certificat.

86. 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.

87. Le Client et son Représentant Légal s'engagent à informer le BE de rattachement de toute modification des informations contenues dans le Certificat et transmettre les pièces justificatives requises, sans délais. ChamberSign France se réserve le droit de révoquer le Certificat conformément au chapitre 9 Révocation du Certificat.

88. 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. 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 et en particulier celles relatives à la protection des données personnelles.

89. 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 de guides et d'une FAQ disponibles sur le site Internet de ChamberSign France : <https://support.chambersign.fr/guides/>.

90. 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.

91. Le responsable de certificats est tenu de vérifier la validité du Certificat et la conformité de son utilisation.

12. OBLIGATIONS RESPONSABLE DE CERTIFICAT

92. Le Responsable de Certificat 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.

93. Le Responsable de Certificat est garant de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.

94. Il 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 et en particulier celles relatives à la protection des données personnelles.

95. Le Responsable de Certificat informe immédiatement ChamberSign France de toute modification concernant les informations contenues dans son Certificat, laquelle entrainera une révocation de son Certificat conformément à l'article 9 Révocation du Certificat. A défaut d'information préalable délivrée par le Responsable de Certificat à ChamberSign France, la responsabilité de ChamberSign France ne pourra pas être engagée au titre d'une information non conforme à la réalité.

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

97. Le Responsable de Certificat s'engage à informer le BE de rattachement de toute modification des informations contenues dans le Certificat, et transmettre les pièces justificatives requises, sans délais. A défaut de se faire, le Client devra s'en charger, conformément à l'article précédent.

98. Le Responsable de Certificat reconnaît être informé des conditions d'installation des Certificats, de guides et de la FAQ disponibles sur le site Internet de ChamberSign France : <https://support.chambersign.fr/guides/>.

99. Le Responsable de Certificat met en œuvre le matériel et les logiciels offrant une sécurité en adéquation avec ses besoins pour l'installation et la protection des Certificats.

100. Le Responsable de Certificat s'engage à respecter les usages autorisés des Bi-clés et des Certificats.

101. Le Responsable 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 mot de passe ou les réponses à ses questions de sécurité pour accéder au processus de révocation.

102. Le Responsable de Certificat protège ses données d'activation et, le cas échéant, les met en œuvre.

103. Le Responsable de Certificat protège l'accès à sa base de Certificats.

104. Le Responsable de Certificat respecte les conditions d'utilisation de sa Clé Privée et du Certificat correspondant.

105. Le Responsable 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).

106. Le Responsable de Certificat s'engage à ne pas transmettre ou partager le Certificat qui lui est attribué ni les codes de protection de ce Certificat (mot de passe et questions de sécurité).

107. Le Responsable de Certificat 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

108. Les Utilisateurs de Certificats sont informés de la nature et de la qualification du Certificat tel qu'indiqué à l'article 2 Définitions, en particulier que celui-ci ne peut être utilisé que pour des services d'Authentification.

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

110. 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.

111. Pour chacun des Certificats de la chaîne de Certification, du Certificat du RCC 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.

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

14. PRIX ET FACTURATION

14.1 Prix

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

114. Les modes de règlement acceptés sont les suivants :

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

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

116. 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.

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

118. 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 maximum de un (1) an (selon la 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 RCC n'ait révoqué le certificat avant sa date



d'anniversaire. Le montant total des factures pourra être supérieur au montant d'un paiement comptant en une seule fois.

119. 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.

120. 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.

121. En cas de non-règlement dans les délais, il sera dû conformément à l'article L 441-10 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 50 Euros. Par exception à ce qui précède, la majoration susvisée sera de 8 points de pourcentage en cas de commande publique. 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.

122. En cas de non-règlement, le Certificat sera révoqué de plein droit par ChamberSign sans ouvrir droit à dommages et intérêts ni remplacements. Les factures restant dues.

14.2 Facturation

123. Les factures originales sont émises par ChamberSign France sous format électronique et sont adressées par email au RCC ou à toute autre adresse email indiquée à cet effet par le RCC lors de la demande de Certificat.

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

125. 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 50 Euros HT en ajoutant 10 Euros HT par certificat (frais d'annulation de chaque facture).

126. 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. RESPONSABILITE

127. ChamberSign France est responsable de la conformité de sa Politique de Certification, avec les exigences émises par les réglementations française et européenne.

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

129. 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 RCC à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats.

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

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

132. 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 RCC, ou du Représentant Légal 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.

133. 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.

134. 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 RCC étant seuls responsables vis-à-vis des tiers du contenu de ces envois.

135. Sans préjudice de l'article 17 Assurance, 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.

136. ChamberSign France n'assume aucun engagement ni responsabilité quant à l'utilisation par le RCC 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.

137. 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.

138. 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.

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

140. Du fait de l'évolution constante de la technologie et des niveaux de sécurités 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.

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

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

16. SECURITE

143. 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 de piratage et s'engage à mettre en œuvre toutes les mesures utiles pour préserver l'intégrité des Certificats et des Bi-Clés.

144. 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.

145. 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.

146. 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.

147. 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

148. 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.

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

18. CONFIDENTIALITE

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

151. 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 que copies, reproductions ou duplications ne sont pas directement liées à l'exécution des présentes.

19. PROPRIETE INTELLECTUELLE

152. 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.

153. A l'exception de l'utilisation des Certificats prévue par les CGU, le Client et le RCC 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, 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.

154. 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.

155. 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.

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

20. DONNEES A CARACTERE PERSONNEL

157. Voir annexe 1

21. RESILIATION DE L'ABONNEMENT

158. Le Client pourra résilier l'abonnement à tout moment et sans cause.

159. Dans ce cas, il ne peut prétendre au remboursement des sommes déjà versées au titre de l'abonnement au service de Certification de ChamberSign France.

160. 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 RCC 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.

161. 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 plein droit, après envoi d'une lettre recommandée avec accusé de réception, visant la présente clause :

- en cas d'expiration de l'ensemble des Certificats n'ayant pas donné lieu à renouvellement ;
- en cas de révocation des Certificats ;
- en cas de non-paiement du prix de l'abonnement.

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

163. 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 à nouveau à signer.

164. En cas de 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.

22. CONSERVATION

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

166. Les journaux d'évènement sont conservés sur site pendant une durée de trente (30) jours dans le cas où le Client a fait une demande en version papier. Après leur génération, ils sont archivés et conservés pendant onze (11) ans.

167. Il appartient au client de conserver un exemplaire du présent Contrat préalablement signé et de transmettre 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 ne sont accessibles qu'aux personnes autorisées. Toute demande de duplicata du dossier d'enregistrement à ChamberSign France sera facturée 50€ HT au Client.

168. Les Certificats et les LCR sont archivés pendant une durée de sept (7) ans après leur expiration.

169. 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.

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

23. NULLITE

171. 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. INTEGRALITE

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

173. 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. REGLEMENT DES LITIGES – TRIBUNAL COMPETENT – LOI APPLICABLE

174. En cas de difficulté de toute nature et avant toute procédure



juridictionnelle, les parties s'engagent à mettre en œuvre une procédure de règlement amiable.

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

176. L'ordre du jour est fixé par la partie qui prend l'initiative de la réunion à l'amiable.

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

178. 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.

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

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

181. 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. ESPACE DE PUBLICATION

182. La politique de certification applicable est publiée à l'adresse suivante :

https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.pdf

183. L'utilisateur peut vérifier l'empreinte du certificat racine sur le site sécurisé <https://pc.chambersign.fr/ca3/index.html> ou en contactant ChamberSign France par téléphone. En cas de compromission des clés d'AC ou de cessation de l'activité, une communication par mail sera transmise individuellement à l'ensemble des RCC en complément de la communication institutionnelle qui sera réalisée.

184. Les points de publication des LCR sont les suivants : http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl et http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.crl

185. Le certificat d'AC est téléchargeable à l'adresse https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_NG_Qualified_eID.cer

27. CONFORMITE

186. Les certificats émis sont qualifiés au niveau eIDAS.

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

188. Les profils de certificats et de LCR sont conformes à la norme ETSI 319 412-4 et 319 412-5.



Annexe 1. Traitement des données à caractère 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 l'Utilisateur. 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 ChamberSign, dans le cadre de la fourniture de nos Services. Les données collectées par ChamberSign sont dès lors 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. Les présentes stipulations ne concernent pas les traitements de données personnelles que ChamberSign peut être amenée à opérer en qualité de sous-traitant.

4. 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, prénoms, etc.), 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.

5. 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 gérer et suivre le cycle de vie de votre certificat (délivrance, renouvellement, révocation, conservation), de gérer l'accès et le fonctionnement de votre Espace Client ou encore de suivre notre relation commerciale.

6. Les informations collectées sont obligatoires. A défaut, ChamberSign France ne pourra pas fournir les services. 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.

7. Les sous-traitants susceptibles d'accéder à vos données à caractère personnel sont les suivants :

- Agence de publicité établie en France, chargé du transfert de la newsletter par mail ;
- Entreprise de Services Numériques (ESN) établie en France chargée d'assurer le premier niveau de support technique ;
- Société d'hébergement informatique établie en France chargée d'héberger le site internet de ChamberSign ;
- Société d'archivage établie en France chargée d'assurer l'archivage des dossiers de demande de certificats pour la durée légale requise ;
- Chambres de Commerces et d'Industrie partenaires de ChamberSign chargées de la vérification des identités, validation des dossiers et délivrances de certificats ;
- Entités publiques et privées partenaires de ChamberSign chargées de la délivrance de certificats pour leurs collaborateurs, clients ou adhérents ;
- Prestataire de service de confiance partenaire de ChamberSign chargé de fournir la signature des parties à la commande de certificats ;

- Prestataire de gestion des chèques chargé de la mise à l'encaissement des règlements par chèques ;
- Prestataire de service de confiance partenaire de ChamberSign chargé de vérifier la validité des documents d'identité.

8. 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.

9. Conformément au Règlement (UE) du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, modifié par le Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 et des présentes CGU, nous conservons vos données 11 (onze) ans à compter de la délivrance du produit.

10. Conformément à la Règlementation en vigueur, vous disposez d'un droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition ainsi qu'un droit à la portabilité de vos données et à définir des directives sur le sort de vos données après votre mort.

11. Afin d'exercer vos droits, vous pouvez nous contacter par courrier 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, étant précisé que pour sécuriser l'authentification, l'envoi d'un mail signé électroniquement est privilégié. 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.

12. En cas de doute raisonnable, ChamberSign se réserve la possibilité de vous demander la fourniture d'une copie de votre pièce d'identité via un moyen sécurisé, étant précisé que cette pièce ne sera pas réutilisée à d'autres fins que votre authentification dans le cadre de la demande d'exercice de vos droits, et ne sera pas conservée au-delà de la durée nécessaire à cette finalité.

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, nous vous invitons expressément à consulter notre [Charte de confidentialité](#), qui fait partie intégrante des présentes Conditions, ou contacter notre Délégué à la Protection des données à l'adresse suivante : rgpd@chambersign.fr.

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>.

1.2. Cookies

1. Lorsque l'Utilisateur visite notre site Internet, des cookies sont envoyés à son ordinateur, sa tablette ou son téléphone mobile sous réserve de l'expression de son consentement depuis la bannière de gestion des cookies affichée sur la première page visitée, et lui permettant d'accepter tous les cookies, de tous les refuser, ou d'en personnaliser la collecte. 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.