CONDITIONS GENERALES D'UTILISATION AC CEGEDIM PERSONNES PHYSIQUES - LCP ET NCP

1. Préambule

Le présent document définit les Conditions Générales d'Utilisation des Certificats émis par l'AC ***CEGEDIM USER ADVANCED CA*** de l'IGC Cegedim. Ces conditions générales sont complétées par les Politiques de Certifications que chaque intervenant de la chaîne de Certification notamment le Porteur, l'Utilisateur, le Représentant Légal du Client ainsi que le Client acceptent pleinement le contenu et reconnaissent être liés par la totalité de leurs dispositions.

Les différents intervenants dans la chaîne reconnaissent disposer de la compétence et des moyens nécessaires pour utiliser les Certificats.

Le Porteur et l'Utilisateur reconnaissent être informés des conditions d'installation du Certificat. A ce titre, le Porteur et l'Utilisateur choisissent le matériel offrant une sécurité en adéquation avec les besoins pour l'installation et la protection des Certificats.

Ce document constitue également les *PKI Disclosure Statements* en présentant les principaux processus proposés pour la gestion des certificats.

2. Contact de l'Autorité de Certification

Par Courrier :

IGC CEGEDIM
Cegedim
137 rue d'Aguesseau
92100 Boulogne-Billancourt

Par courriel :

igc@cegedim.fr

3. Définitions

Les termes utilisés dans les présentes Conditions Générales d'Utilisation commençant par une majuscule, indifféremment utilisés au singulier ou au pluriel, ont, sauf stipulation contraire, la signification qui leur est donnée ci-dessous :

Autorité de Certification (AC) : Entité responsable de la génération et des listes de révocation des Certificats de l'Autorité de Certification ***CEGEDIM USER ADVANCED CA***, selon les engagements énoncés dans la Politique de Certification de cette Autorité de Certification.

Autorité d'Enregistrement (AE) : Entité responsable de la vérification d'identité du Porteur, de l'établissement de la demande de certificat, et le cas échéant, de la conservation de pièces justificatives du Porteur.

Biclé : désigne la paire constituée d'une Clé Privée et d'une Clé Publique.

Certificat : Attestation électronique délivrée par l'AC au Porteur et que celui-ci utilise pour signer. Le Certificat est décrit dans la Politique de Certification de l'AC.

Clé Privée : désigne la clé que le Porteur doit maintenir confidentielle.

Clé Publique : désigne la clé rendue publique et qui est utilisée pour vérifier la signature d'une donnée reçue.

Client : Société cliente de Cegedim qui peut lancer de nouvelles cérémonies de signatures et y inviter des personnes physiques à signer des documents.

Compromission : Comprend à la fois la compromission système qui désigne l'activité d'un code ou d'un acteur malveillant sur une machine du système d'information résultant en sa prise de contrôle partielle ou totale. La compromission renvoie également à la divulgation ou à la suspicion de divulgation d'informations confidentielles ou non ou à l'altération de l'intégrité d'un Certificat.

Conditions Générales d'Utilisation (CGU) : Désigne les présentes conditions générales d'utilisation.

Infrastructure de Gestion des Clés (IGC) : Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs.

OID : désigne le système d'identification des entités physiques ou virtuelles et composés d'une suite de nombre entiers.

Politique de Certification (PC) : Document présentant les engagements et les pratiques de l'Autorité de Certification et de ses partenaires pour fournir les services de gestion des certificats.

Porteur : Personne physique invitée à signer électroniquement des documents en son nom propre, dans le cadre d'une cérémonie de signature organisée sur un service Cegedim.

Représentant Légal : Désigne le Représentant Légal du Client

Utilisateur : Désigne toute personne physique ou morale utilisant un Certificat, par exemple pour vérifier la signature d'un document.

4. Références documentaires

[eIDAS] : Règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur

[ETSI] : Norme *ETSI EN 319 411-1 : Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements*

[CNIL] : Commission nationale de l'informatique et des libertés

[RGPD] : Règlement européen n°2016/679 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

[PC] : Politique de Certification et Déclarations de Pratiques de Certification de l'AC ***CEGEDIM USER ADVANCED CA,*** disponible sur le site Cegedim

5. Objet

Les présentes CGU ont pour objet, en combinaison avec la PC, de définir le cadre et les conditions dans lesquelles le Client pourra utiliser les Certificats émis par l'AC.

6. Conditions de validité et d'application

La dernière version des CGU est disponible sur le site public de l'AC.

Les présentes CGU sont opposables au Client, au Porteur, et au Responsable Légal dès leur signature ou dès la première utilisation du Certificat. L'Utilisateur reconnait que l'utilisation du Certificat entraîne l'acceptation des nouvelles CGU par le Client. Le Client se porte-fort du respect des CGU par l'Utilisateur du Certificat.

Les présentes CGU sont considérées comme conclues et sont opposables au Client pendant toute la durée de vie du Certificat à compter de la date d'émission de ce dernier.

Le Client est réputé avoir accepté les nouvelles CGU s'il continue à utiliser le Certificat après la mise à jour de ces dernières. Cette acceptation est considérée comme étant pleine et entière.

7. Modalités de demande de certificat

7.1. Demande de Certificat

Les modalités de demande, de vérification ainsi que les cas de rejets et les conditions de délivrance du Certificat sont décrites dans la PC « AC Cegedim Personnes Physiques - LCP et NCP » présente sur le site et à l'adresse : https://psco.cegedim.com/documents.html

7.2. Renouvellement du Certificat

Les Certificats ont une durée de validité limitée et ne peuvent pas être renouvelés. Pour continuer à bénéficier de la couverture, le Client doit générer un nouveau Certificat dans les conditions et critères en vigueur à la date de délivrance du nouveau certificat.

7.3. Modification du Certificat

Le Certificat ne peut être modifié. En cas de modification des informations contenues dans le Certificat, le Certificat initial devra être révoqué et le Client devra procéder à une nouvelle demande de Certificat.

8. Niveau et usage des certificats

Les Certificats, émis par l'AC ***CEGEDIM USER ADVANCED CA,*** sont des certificats avancés de signature électronique à la volée au sens du règlement eIDAS. Ils sont conformes aux niveaux suivants de la norme [ETSI] :

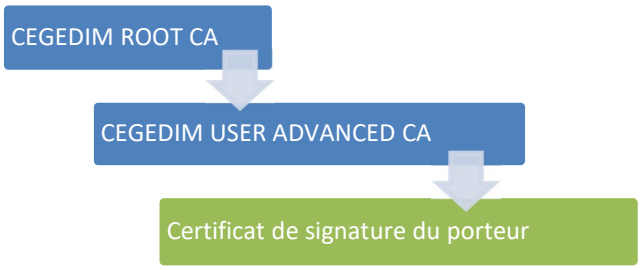
Type de certificat	Niveau eIDAS OID de l'ETSI	OID de la PC OID des CGU
Certificat de signature pour une personne physique enregistrée en face à face	Niveau NCP 0.4.0.2042.1.1	PC : 1.3.6.1.4.1.142057.10.4.1.1.1 CGU : 1.3.6.1.4.1.142057.10.4.1.2.1
Certificat de signature pour une personne physique enregistrée en ligne	Niveau LCP 0.4.0.2042.1.3	PC : 1.3.6.1.4.1.142057.10.4.2.1.1 CGU : 1.3.6.1.4.1.142057.10.4.1.2.1

Les Politiques de Certification sont publiées à l'adresse suivante :
http://psco.cegedim.com/CPS

La conformité des Politiques de Certification identifiées ci-dessus à la norme [ETSI] a été auditée par un organisme dûment accrédité au niveau européen pour réaliser des audits de certification eIDAS. Ces audits sont menés au minimum tous les deux ans.

9. Chaîne de certification

La chaîne de certification des certificats de signature d'un Porteur est la suivante :



Les certificats des autorités de certification sont publiés sur :

http://psco.cegedim.com/CRT

10. Modalités d'obtention

Le Certificat est demandé par le Porteur durant une cérémonie de signature de documents électroniques.

- Le Porteur présente une pièce d'identité officielle à l'Autorité d'Enregistrement (en face à face ou via une copie transmise en ligne selon le niveau du certificat), qui en vérifie l'authenticité et la validité ;
- Un code d'authentification à usage unique est envoyé par courriel ou sur le téléphone mobile du Porteur puis contrôlé par l'AE pour renforcer son authentification ;
- Après acceptation par le Porteur des présentes CGU, un Certificat lui est émis par l'Autorité de Certification. Ce Certificat est utilisé sur la plateforme Cegedim exclusivement pour signer les documents objets de la cérémonie de signature.

L'acceptation du Certificat émis est tacite, dès sa génération, du fait de la vérification préalable par le Porteur de ses données d'identité et de l'acceptation explicite des présentes CGU.

Le Certificat de signature du Porteur n'est pas publié, il est transmis au Porteur dans le ou les documents signés.

11. Modalités de révocation et de suspension

Le Porteur ne peut pas demander la révocation de son certificat étant donné que les certificats sont éphémères (d'une durée de validité limitée à 30 minutes) et que la clé privée est détruite dès la signature terminée.
La suspension de Certificat n'est pas autorisée.

12. Modalités de vérification des certificats

L'Utilisateur d'un Certificat de Porteur est tenu de vérifier, avant son utilisation, la validité des Certificats de l'ensemble de la chaîne de certification correspondante. En particulier :

- Les dates de validité des certificats, inscrites dans les certificats ;
- La chaîne de certification grâce aux certificats d'AC disponibles sur http://psco.cegedim.com/CRT ;
- Le statut de révocation grâce aux CRL disponibles sur http://psco.cegedim.com/CRL.

En cas de compromission de la clé privée d'AC, outre l'information de cet incident sur le site public de l'AC, tous les certificats émis par l'AC concernée devront être considérés comme révoqués à la date de compromission annoncée. Une ultime CRL sera générée avec la clé compromise (pour permettre aux outils de traiter ce cas technique), et la CRL sera horodatée et signée (signature détachée) par le certificat de l'AC racine afin de fournir une preuve d'authenticité (non technique).

13. Conditions et limites d'usage

L'utilisation de la Clé Privée du Porteur et du Certificat associé est strictement limitée à la signature à la volée de documents, pour la durée de la session de signature en cours.

Les Utilisateurs du Certificat ont la possibilité de vérifier la validité de la signature électronique des documents grâce à leur Clé Publique.

Le Certificat généré n'est utilisable que pour la cérémonie de signature pour laquelle il a été demandé. Le Certificat est valide pour une période de 30 minutes et ne peut pas être renouvelé. Si le Certificat expire avant la signature de tous les documents par le Porteur, un nouveau certificat devra être est émis pour les signatures restantes.

Tout usage est interdit.

De même, le client s'interdit d'utiliser à d'autres fins qu'à des fins de test les Certificats de test émis par l'AC. Ces Certificats de test sont clairement identifiés par le préfixe ou le suffixe « TEST » placé dans le champ CN.

14. Procédure de vérification des Certificats

La procédure de vérification des Certificats est détaillée dans la PC.

15. Obligations des Porteurs

La fiabilité de la signature électronique et des certificats émis demande le respect par le Porteur des obligations suivantes :

- Communiquer des informations exactes, complètes, pertinentes et à jour à l'Autorité d'Enregistrement ;
- Vérifier ses données d'identité dans la demande de Certificat ;
- Consentir à la conservation des informations aux fins de gérer les Certificats dans les conditions prévues par les lois et règlements applicables ;
- Accepter que le moteur de signature Cegedim génère, utilise puis détruise la clé privée en son nom et selon les modalités définies dans la Politique de Certification (Les bi-clés des porteurs sont des clés RSA de taille minimale de 2048 bits ; au plus tard le 1er janvier 2026, la taille minimale des clés RSA sera de 3072 bits) ;
- Assurer la sécurité et le contrôle exclusif du compte de messagerie ou du téléphone mobile sur lequel il reçoit le code d'authentification à usage unique ;
- Accepter la conservation par l'AE et l'AC du dossier d'enregistrement et des journaux d'événements relatifs à son Certificat, afin de les produire comme preuve, le cas échéant en justice ;
- Protéger l'accès à sa base de Certificats ;
- Ne plus utiliser la clé privée correspondante après avoir été informé de la révocation de son certificat ou de la compromission de l'AC émettrice ;
- Consentir à l'utilisation de ses informations personnelles dans le cadre de l'exécution des présentes CGU et de la Politique de Certification associée ;
- Respecter, plus largement, les obligations qui lui incombent dans le cadre des présentes CGU et de la Politique de Certification associée.

16. Obligations de l'Autorité d'Enregistrement et de l'Autorité de Certification

L'Autorité d'Enregistrement et l'Autorité de Certification s'engagent à fournir des prestations de certification électronique conformes à la Politique de Certification et aux réglementations en vigueur. En particulier :

- L'AE vérifie avec attention les données d'identité du Porteur ;
- L'AC fournit les moyens nécessaires à la vérification des Certificats des Porteurs, disponibles 24/24 et 7/7, avec un taux de disponibilité annuel de 99.5% ;
- L'AE et l'AC conservent les informations qui pourraient s'avérer nécessaires à titre de preuve de bon fonctionnement de son service et d'intégrité des données utilisées ;
- L'AE et l'AC respectent la protection des données à caractère personnel (en particulier le règlement RGPD) dans l'ensemble de leurs activités.

17. Conservation des preuves

L'AE et l'AC conservent les dossiers d'enregistrement des Porteurs ainsi que des journaux d'événements pour une période de 10 ans à compter de l'émission du Certificat du Porteur. Le dossier d'enregistrement intègre les informations du document d'identité présenté par le porteur et les résultats de vérification par l'opérateur de l'AE ou le système automatisé de vérification des titres d'identité.
Ces données pourront notamment être utilisées à titre de preuve en justice.

L'AE et l'AC garantissent l'intégrité et la confidentialité de ces données sur toute leur période de conservation, en respect de la règlementation de la protection des données à caractère personnel.

18. Fin de vie de l'AC

Cegedim dispose et maintient à jour un plan de cessation ou de transfert d'activité de ses services de confiance afin de garantir aux porteurs et utilisateurs des certificats un impact minimal. En particulier, ce plan prévoit :

- En cas d'expiration ou de cessation d'activité de l'AC :
  - La révocation de l'ensemble des certificats non expirés émis par cette AC ;
  - La génération et la publication d'une dernière liste de révocation ayant comme date de fin de validité le 31 décembre 9999, 23h59m59s ;
  - Après avoir généré sa dernière CRL, la clé privée de l'AC sera détruite de façon définitive.
  - En cas de compromission de la clé privée d'une AC, la dernière CRL émise est publiée accompagnée d'une empreinte SHA-256 afin d'en garantir l'intégrité et l'origine.
- Cegedim s'engage à prévenir tous ses clients et les porteurs de certificats (excepté les porteurs de certificats éphémères) par mail et par un message sur son site Internet au minimum au moins 3 mois avant la date effective de cessation d'activité de l'AC (sauf cas d'incident de sécurité nécessitant une réaction plus rapide).

En cas de cessation d'activité de Cegedim, y compris après un éventuel transfert d'activité, une solution technique sera trouvée afin que les certificats et CRL puissent être téléchargées sur les URL prévues.

19. Limite de responsabilité

Cegedim est soumise à une obligation générale de moyens.

Cegedim ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des Certificats, des CRL.
La responsabilité de Cegedim ne pourra être engagée pour tout dommage causé par des informations erronées, inexactes ou incomplètes contenues dans les Certificats si ces erreurs, inexactitudes ou omission résultent notamment des informations communiquées par le Porteur ou le Client.

La responsabilité de Cegedim ne pourra être engagée en cas d'informations inexactes incomplètes ou non mises à jour.
La responsabilité de Cegedim ne pourra être engagée en cas d'interruption ou de disfonctionnement des services et applications du Porteur, du Responsable Légal ou de l'Utilisateur du Certificat.

De plus, dans la mesure des limitations de la loi française, Cegedim ne saurait être tenu responsable :

- d'aucune perte financière ;
- d'aucune perte de données ;
- d'aucun dommage indirect lié à l'utilisation d'un Certificat ;
- de l'utilisation de la Clé Privée du Porteur ;
- de l'utilisation non autorisée ou non conforme faite par le Porteur du Certificat, l'Utilisateur ou le Responsable de Certificat.
-

En toute hypothèse, la responsabilité de Cegedim sera limitée, tous faits générateurs confondus et pour tous préjudices confondus, au montant payé à Cegedim pour l'accès au service de signature et ce, dans le respect et les limites de la loi applicable.

Les limitations ou exclusions de responsabilité contenues au présent article ne s'appliquent pas aux dommages corporels ni à ceux ayant pour cause une faute lourde.

20. Protection des données à caractère personnel

Le Groupe Cegedim respecte, pour le traitement et la protection des données à caractère personnel, la loi française no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi no 2004-801 du 6 août 2004 [CNIL], et au Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 [RGPD].

Les données personnelles ne sont jamais utilisées, sans le consentement exprès et préalable de la personne, à d'autres fins que celles définies :

- Dans la politique et les pratiques du service ;
- Dans l'accord de souscription ou tout accord contractuel.

Les données personnelles peuvent être mis à la disposition de la justice en cas de besoin pour servir de preuve dans le cadre d'une procédure judiciaire.

21. Propriété Intellectuelle

Chacune des Parties et des utilisateurs du Certificat garantissent avoir la libre disposition des marques, noms et tout autre signe distinctif destinés à être utilisés dans le cadre des présentes CGU.

Les présentes CGU n'emportent aucune cession d'aucune sorte de droits de propriété intellectuelle sur tout ou partie des éléments appartenant à l'AC, à l'AE ou tout intervenant de la chaîne de certification.

22. Conditions d'indemnisation

Sans objet pour le Porteur du Certificat de signature.

23. Sécurité

Les conditions de mise à jour de l'analyse des risques et de notification à l'Agence Nationale de la Sécurité des Systèmes d'Information et à la Commission Nationale de l'Informatique et des Libertés sont décrites dans le document « mesures de sécurité communiques aux AC Cegedim » disponible sur le site de Cegedim.

En cas d'atteinte à la sécurité ou de perte d'intégrité qui est susceptible de porter préjudice au Client ou au Porteur du Certificat, l'AC s'engage à notifier dans les meilleurs délais à la personne physique ou morale l'atteinte à la sécurité ou la perte d'intégrité.

24. Loi applicable et règlement des litiges

Pour toute réclamation, le Porteur peut s'adresser à l'AC par courriel à l'adresse suivante: **sales.etrust@cegedim.com**

La Politique de Certification, les présentes CGU et l'ensemble des documents contractuels sont soumis à la législation et à la réglementation en vigueur sur le territoire français.

En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de Paris.

25. Conformité à la règlementation

L'Autorité d'Enregistrement et l'Autorité de Certification s'engagent à respecter l'ensemble des réglementations en vigueur pour les services qu'elles proposent, en particulier :

- Le règlement eIDAS ;
- Le règlement RGPD ;
- La propriété intellectuelle.

26. Liens utiles

Le Certificat AC Cegedim Root CA est disponible sur le Site et à l'adresse suivante : https://psco.cegedim.com/CRT/CEGEDIMROOTCA.crt

Le Certificat racine de l'AC Cegedim Personnes Physiques - LCP et NCP est téléchargeable sur le site et à l'adresse suivante : https://psco.cegedim.com/documents.html