CONDITIONS GENERALES D'UTILISATION AC CEGEDIM HORODATAGE QUALIFIE

1. Préambule

Le présent document définit les Conditions Générales d'Utilisation des Certificats émis par l'AC ***CEGEDIM TIMESTAMP QUALIFIED 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 / Autorité d'Enregistrement

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 de la révocation des Certificats de l'Autorité de Certification ***CEGEDIM TIMESTAMP QUALIFIED 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 et de l'Entité, de la validation des demandes de certificat ou de révocation, 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 à l'Entité et que celle-ci utilise pour créer des cachets électroniques (ici pour des jetons d'horodatage). 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.

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.

Entité : Société ou administration cliente de Cegedim qui a contractualisé l'approvisionnement de certificats de cachet pour des services qu'elle propose.

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 ou RCCS : Personne physique Responsable de Certificat de Cachet Serveur (ici des certificats d'horodatage) à qui est remis le Certificat d'horodatage de l'Entité, délivré sous la responsabilité de l'Autorité d'Enregistrement.

Service d'horodatage électronique : Service de confiance qui permet d'identifier l'heure exacte d'un évènement, tout en garantissant que l'élément horodaté n'a pas été modifié après l'enregistrement. Il est décrit comme étant « qualifié » lorsque le service respecte des exigences de sécurité renforcées.

Utilisateur : Désigne toute personne physique ou morale utilisant un Certificat, par exemple pour vérifier un cachet électronique apposé sur 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 TIMESTAMP QUALIFIED CA,*** disponible sur le site Cegedim

5. Porteurs des certificats (RCCS)

Les Porteurs de Certificat sont des personnes physiques Responsable de Certificat de Cachet Serveur (RCCS) qui sont responsables de la demande, du renouvellement et de la révocation des Certificats d'horodatage de l'Entité. Les RCCS agissent au nom de l'Entité à laquelle le certificat est délivré.

Dans le cadre de l'AC ***CEGEDIM TIMESTAMP QUALIFIED CA***, seule l'entité Cegedim peut obtenir un certificat d'horodatage pour l'une des unités d'horodatage de son service qualifié d'horodatage.

6. Objet

Les présentes CGU ont pour objet, en combinaisons avec la PC, de définir le cadre et les conditions dans lesquelles le service d'horodatage pourra être utilisé.

7. 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 à tous les demandeurs, les utilisateurs et les personnes ayant souscrit au service d'horodatage.

8. Modalités d'émission et de délivrance des certificats

8.1. Demande de Certificat

Les modalités d'émission et de délivrances du certificat sont décrites dans la PC « AC Cegedim Horodatage-QCP-l » disponible sur le Site de Cegedim et à l'adresse suivante : http://psco.cegedim.com/CPS

8.2. Renouvellement du Certificat

Le renouvellement d'un Certificat peut être demandé trois (3) mois avant son expiration dans les conditions fixées par la PC.

8.3. 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.

9. Niveau et usage des certificats

Les Certificats, émis par l'AC ***CEGEDIM TIMESTAMP QUALIFIED CA,*** sont des certificats qualifiés d'horodatage destinés à l'une des unités d'horodatage du service qualifié d'horodatage de Cegedim. Ils sont conformes aux niveaux suivants de la norme [ETSI] :

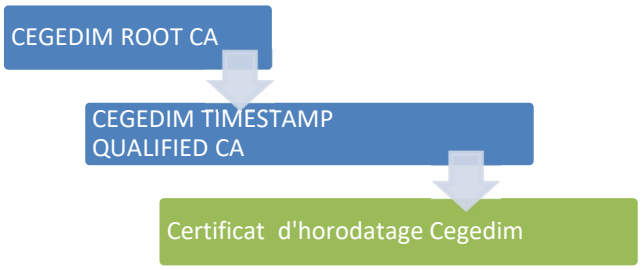
Type de certificat	Niveau eIDAS OID de l'ETSI	OID de la PC OID des CGU
Certificat qualifié d'horodatage pour un service d'horodatage Cegedim	Niveau QCP-l 0.4.0.194112.1.1	PC : 1.3.6.1.4.1.142057.10.7.1.1.1 CGU : 1.3.6.1.4.1.142057.10.7.1.2.1

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. La qualification des certificats est délivrée par l'ANSSI après l'évaluation du niveau de sécurité des processus de délivrance et de gestion de l'AC.

10. Chaîne de certification

La chaîne de certification des certificats d'horodatage est la suivante :



Les certificats des autorités de certification sont publiés sur :

http://psco.cegedim.com/CRT

11. Modalités d'obtention

Le Certificat est demandé par le Porteur durant un face à face avec l'Autorité d'Enregistrement :

- Le Porteur présente une pièce d'identité officielle, une pièce justificative attestant de l'existence de l'entité (le Client) à laquelle sera rattaché le certificat, ainsi qu'une preuve de son habilitation à effectuer cette demande ;
- L'AE vérifie l'authenticité et la validité des documents présentés ;
- Le Porteur accepte les présentes CGU et les signe avec sa demande de certificat ;
- Le Porteur fournit une requête de certificat (CSR) qu'il a générée sur un dispositif cryptographique matériel sécurisé de l'une de ses unités d'horodatage ;
- Après validation de la demande par l'AE, l'Autorité de Certification délivre au porteur, sans délai, un Certificat d'horodatage en réponse à la requête.

Le Porteur accepte formellement le Certificat qui lui est remis par l'AE. Le Porteur peut révoquer le Certificat s'il souhaite le refuser avant de l'utiliser.

Le Certificat d'horodatage du Porteur n'est pas publié.

12. Modalités de révocation et de suspension du Certificat

12.1. Les modalités de révocation du Certificat

Le Porteur doit demander sans délai la révocation selon les modalités prévues par la PC dans les cas suivants :

- Découverte d'une erreur dans son dossier d'enregistrement ou son Certificat ;
- Refus du Certificat ;
- La clé privée est suspectée de compromission, est compromise ou est perdue ;
- Les données d'activation de la clé privée sont suspectées de compromission, sont compromises ou ont été perdues.
- La cessation d'activité du Client
- Le départ de la société du Porteur ou la cessation de son activité
- Le service d'horodatage est interrompu par Cegedim.

La révocation d'un Certificat peut aussi être demandée par l'AE ou l'AC au moins dans les cas suivants :

- L'AE ou l'AC est informée que l'une des causes de révocation ci-dessus est avérée ;
- Les modalités d'utilisation du certificat ou les obligations du porteur n'ont pas été respectées ;
- Une rupture technologique nécessite de procéder à la génération de nouvelles biclés ;
- L'AC doit être révoquée.

La révocation d'un Certificat peut être demandée par le porteur ou le représentant légal de l'entité par courrier à l'AE ou l'AC. La demande doit identifier le certificat à révoquer (nom du service et de l'entité, dates de validité), être signée et comporter un justificatif d'identité du demandeur.

12.2. Les modalités de suspension du Certificat

La suspension du Certificat n'est pas permise.

13. 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.

L'AC informe les Utilisateurs de certificats que les certificats révoqués sont conservés dans la CRL y compris après la fin de leur période de validité.
En cas de fin de vie de l'AC, celle-ci produira une ultime LCR, avec comme fin de validité le 31 décembre 9999, 23h59m59s.
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).

14. Conditions et limites d'usage

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la signature de jetons d'horodatage électronique du service qualifié d'horodatage Cegedim telle que l'extension des certificats le prévoit.

Les Utilisateurs de ces Certificats peuvent vérifier l'origine et l'intégrité des données qui ont été scellées avec le Certificat délivré à l'Entité.

Tout autre 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 tets sont clairement identifiés par le préfixe ou le suffixe « TEST » placé dans le champ CN.

15. Procédure de vérification des Certificats

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

16. Obligations des Demandeurs et des Porteurs

La fiabilité des jetons d'horodatage 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 et l'informer de toute modification éventuelle de celles-ci ;
- Disposer de connaissances techniques qui lui permettent de vérifier l'adéquation à son besoin du Certificat ;
- Consentir à la conservation des informations aux fins de gérer les Certificats dans les conditions prévues par les lois et règlements applicables :
- Vérifier les données d'identification du service et de l'entité dans le demande de Certificat ;
- Générer sa biclé (clé RSA de taille minimale de 4096 bits) dans un dispositif cryptographique sécurisé et selon les modalités définies dans la Politique de Certification ;
- Assurer la sécurité et le contrôle exclusif de son dispositif cryptographique ;
- Garantir la confidentialité des données d'activation ;
- 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 ;
- Respect les limites d'usage de son certificat ;

- Demander sans délai la révocation de son Certificat s'il constate une erreur, une fraude ou une autre raison de révocation concernant son Certificat ;
- 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 ;
- Respecter, plus largement, les obligations qui lui incombent dans le cadre des présentes CGU et de la Politique de Certification associée.

17. 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 et de l'Entité ;
- L'AE s'assure que le certificat est destiné au service d'horodatage qualifié de Cegedim ;
- 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 demandent la révocation du Certificat dès qu'un événement anormal, précisé dans la Politique de Certificat, a été constaté ;
- 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 conformément le règlement RGPD) dans l'ensemble de leurs activités.

18. 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. 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.

19. 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.

20. Limite de responsabilité

Cegedim est soumis 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'activation, des Certificats, des CRL.

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 Demandeur, 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 ;
- d'aucun autre dommage.
- 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.

21. 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.

22. 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 tout autre intervenant de la chaîne de certification.

23. Conditions d'indemnisation

Les conditions d'indemnisation sont régies par les conditions de vente avec le Client.

24. 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 communes 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.

25. Loi applicable et règlement des litiges

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.

26. 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.

27. 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 Horodatage -QCP-l : https://psco.cegedim.com/CRT/CEGEDIMTIMESTAMPQUALIFIEDCA.crt