CONDITIONS GENERALES D'UTILISATION AC CEGEDIM ENTITES - QCP-L ET QCP-L-QSCD

1. Préambule

Le présent document définit les Conditions Générales d'Utilisation des Certificats émis par l'AC ***CEGEDIM ENTITY QUALIFIED CA*** de l'IGC Cegedim.

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 ENTITY 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. Le Certificat est décrit dans la Politique de Certification de l'AC.

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.

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.

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.

Liste de Certificat Révoqué (LCR ou CRL) : Liste de certificats qui ont été révoqués avant leur date d'expiration. Cette liste est établie et gérée par l'AC.

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 à qui est remis le Certificat de cachet de l'Entité, délivré sous la responsabilité de l'Autorité d'Enregistrement.

Représentant Légal : Désigne le Représentant Légal du Client

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 ENTITY 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 de cachet de l'Entité. Les RCCS agissent au nom de l'Entité à laquelle le certificat est délivré.

6. Niveau et usage des certificats

Les Certificats, émis par l'AC ***CEGEDIM ENTITY QUALIFIED CA,*** sont des certificats qualifiés de cachet. Ils sont conformes aux niveaux suivants de la norme [ETSI] :

Label	Type de certificat	Niveau eIDAS OID de l'ETSI	OID de la PC
Certificat QCP-l sur HSM client	Certificat qualifié de cachet pour une personne morale qui génère sa clé privée	Niveau QCP-l 0.4.0.194112.1.1	1.3.6.1.4.1.142057. 10.3.1.1.1
Certificat QCP-l-qscd sur HSM distant	Certificat qualifié de cachet qualifié sur HSM pour une personne morale qui génère sa clé privée sur un QSCD (qui lui appartient ou qui est hébergé chez un TSP qualifié pour cela)	Niveau QCP-l-qscd 0.4.0.194112.1.3	1.3.6.1.4.1.142057. 10.3.2.1.1

Label	Type de certificat	Niveau eIDAS OID de l'ETSI	OID de la PC
Certificat QCP-l sur HSM de l'AC	Certificat qualifié de cachet pour une personne morale confiant à l'AC la gestion de sa clé privée	Niveau QCP-l 0.4.0.194112.1.1	1.3.6.1.4.1.142057. 10.3.3.1.1
Certificat QCP-l-qscd sur puce client	Certificat qualifié de cachet qualifié remis sur puce qualifiée pour une personne morale qui y génère sa clé privée	Niveau QCP-l-qscd 0.4.0.194112.1.3	1.3.6.1.4.1.142057. 10.3.4.1.1

Au sens du règlement eIDAS :

- Les certificats de niveau QCP-l permettent de créer des cachets avancés sur la base de certificats qualifiés ;
- Les certificats de niveau QCP-l-qscd permettent de créer des cachets qualifiés.

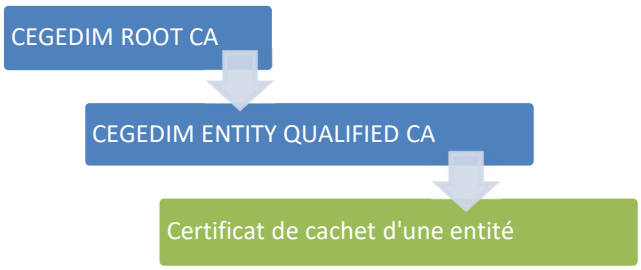
Les Politiques de Certification sont publiées à l'adresse suivante :

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.

7. Chaîne de certification

La chaîne de certification des certificats de cachet est la suivante :



Les certificats des autorités de certification sont publiés sur :

http://psco.cegedim.com/CRT

8. Modalités d'obtention

Le Certificat est demandé par le Porteur à une Autorité d'Enregistrement selon l'une des modalités suivantes :

- Durant un face à face physique avec un opérateur d'enregistrement qui vérifie l'identité du Porteur sur la base de la présentation d'une pièce d'identité officielle ;
- Sur le portail de l'Autorité d'Enregistrement, qui dirige le porteur vers un service de vérification d'identité à distance d'un prestataire certifié PVID au niveau substantiel ;
- Sur le portail de l'Autorité d'Enregistrement, qui demande au Porteur de s'identifier en utilisant un Moyen d'identification électronique de niveau de garantie substantiel.

Le processus de demande se poursuit de la façon suivante :

- 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 ;
- Selon le cas :
  - PC d'OID 1.3.6.1.4.1.142057.10.3.1.1.1 : Le Porteur fournit une requête de certificat (CSR) qu'il a générée sur un dispositif cryptographique matériel sécurisé ;
  - PC d'OID 1.3.6.1.4.1.142057.10.3.2.1.1 : Le RCCS fournit une requête de certificat (CSR) qu'il a générée sur un dispositif cryptographique matériel de niveau QSealCD, le modèle du QSealCD utilisé et la preuve de génération de la clé privée sur celui-ci ;
  - PC d'OID 1.3.6.1.4.1.142057.10.3.3.1.1 : L'AC génère pour le compte du RCCS une bi-clé sur son propre dispositif cryptographique ainsi que la requête de certificat (CSR) correspondante. Le RCCS convient avec l'AC du moyen d'authentification forte qui sera utilisé pour l'activation du cachet ;
  - PC d'OID 1.3.6.1.4.1.142057.10.3.4.1.1 : Le RCCS reçoit un support de puce cryptographique de niveau QSealCD sur laquelle est générée sa clé privée.
- Après validation de la demande par l'AE, l'Autorité de Certification délivre au RCCS, sans délai, un Certificat de cachet en réponse à la requête.

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

Le Certificat de cachet du RCCS n'est pas publié.

9. Modalités de révocation

Le RCCS doit demander sans délai la révocation 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.
- Le service de cachet de l'entité est interrompu par l'Entité.

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 RCCS 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 RCCS ou le représentant légal de l'entité par courrier électronique à l'AE ou l'AC en utilisant le formulaire disponible sur le site https://psco.cegedim.com/documents.html. La demande doit identifier le certificat à révoquer (numéro de série, dates de validité), être signée manuscritement et comporter un justificatif d'identité du demandeur.

Le demandeur est susceptible d'être contacté par l'AE dans les 24 heures suivant sa demande (par courriel ou téléphone), pour des vérifications complémentaires. Le demandeur doit donc s'assurer d'être joignable aux coordonnées indiquées dans son dossier d'enregistrement durant cette période. Dans le cas contraire, sa demande sera possiblement rejetée par l'AE.

10. Modalités de vérification des certificats

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante, en remontant jusqu'aux certificats de la liste de confiance européenne (https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls).

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 CRL, ayant pour date de 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).

Le demandeur est susceptible d'être contacté par l'AE dans les 24 heures suivant sa demande (par courriel ou téléphone), pour des vérifications complémentaires. Le demandeur doit donc s'assurer d'être joignable aux coordonnées indiquées dans son dossier d'enregistrement durant cette période. Dans le cas contraire, sa demande sera possiblement rejetée par l'AE.

11. Limites d'usage

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la création de cachets électroniques.

Tout autre usage est interdit.

12. Obligations des Porteurs

La fiabilité des cachets électroniques et des certificats émis demande le respect par le Porteur des obligations suivantes :

- Communiquer des informations exactes, fiables, complètes et à jour à l'Autorité d'Enregistrement et l'informer de toute modification éventuelle de celles-ci ;
- Vérifier les données d'identification du service et de l'entité dans le demande de Certificat ;
- Garantir la confidentialité des données d'activation ;
- Informer l'AE en cas de demande de certificat ou de révocation non suivie d'un « e-mail » de confirmation
- Respect les limites d'usage de son Certificat ;
- Vérifier régulièrement la LCR pour garantir la validité de son Certificat ;
- Demander sans délai la révocation de son Certificat en cas de réalisation de l'un des cas prévus à l'article 9 des présentes CGU ;
- Accepter la conservation par l'AE et l'AC du dossier d'enregistrement et des journaux d'événements relatifs à son Certificat selon les modalités prévues par l'article 14 des présentes CGU
- À 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 ;
- Respecter, plus largement, les obligations qui lui incombent dans le cadre des présentes CGU et de la Politique de Certification associée.

– Certificat QCP-l sur HSM client :
  - 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 ;
– Certificat QCP-l-qscd sur HSM distant :
  - Générer sa biclé (clé RSA de taille minimale de 4096 bits) dans un dispositif cryptographique qualifié QSealCD et selon les modalités définies dans la Politique de Certification ;
  - Fournir avec la demande de certificat le modèle du QSealCD utilisé et la preuve de génération de la clé privée sur celui-ci (procès-verbal de cérémonie des clés, contenu du QSealCD, …) ;
  - Assurer la sécurité et le contrôle exclusif sur sa biclé (données d'activation) ;
  -

– Certificat QCP-l sur HSM de l'AC :
  - Accepter la génération, la conservation et l'utilisation de la clé privée de son certificat de cachet dans les conditions décrites par la Politique de Certification ;
  - S'authentifier de manière sécurisée auprès de l'AC pour utiliser sa clé privée de cachet. Les méthodes d'authentification acceptées par l'AC sont des mécanismes d'authentification forte et dynamique comprenant :
    - L'authentification par un certificat TLS accepté et enregistré auprès de l'AC ;
    - L'authentification par un fournisseur d'identité accepté et enregistré auprès de l'AC ;
  - Assurer la sécurité du ou des moyens d'authentification utilisés ainsi que de leurs données d'activation ;

– Certificat QCP-l-qscd sur puce client :
  - Contrôler la génération de la clé privée sur le support cryptographique qui lui est remis par l'AC (et en particulier s'assurer qu'il s'agit d'une clé RSA de taille minimale de 4096 bits);
  - Assurer la sécurité et le contrôle exclusif de son dispositif cryptographique ;
  - Garantir la confidentialité de son code PIN et des réponses aux questions de sécurité qu'il a choisie.

13. 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'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 le règlement UE n°2016/679 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 du 27 avril 2016 dit « RGPD » et la loi Informatique et libertés du 6 janvier 1978 modifiée) dans l'ensemble de leurs activités.

14. 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.

15. 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.

16. Limite de responsabilité

Cegedim, est soumise à une obligation générale de moyen.

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 pour tout dommage causé par des informations erronées, inexactes ou incomplètes contenues dans les Certificats si ces erreurs, inexactitudes ou omission résultant des informations communiquées par le Porteur.

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 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.

17. Propriété Intellectuelle

Le Porteur convient que les Certificats sont des documents électroniques protégés par la propriété intellectuelle. Le Porteur s'engage à ne pas reproduire, distribuer ou modifier les Certificats électroniques sans autorisation écrite préalable. Le Porteur s'engage à respecter les droits de propriété intellectuelle de l'émetteur du Certificat et à ne pas utiliser les Certificats en violation de ces droits.

18. 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.

19. Conditions d'indemnisation

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

20. Loi applicable et règlement des litiges

Pour toute réclamation, le RCCS 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.

21. 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.