CONDITIONS GENERALES D'UTILISATION AC CEGEDIM PERSONNES PHYSIQUES - QCP-N-QSCD

1. Préambule

Le présent document définit les Conditions Générales d'Utilisation des Certificats émis par l'AC ***CEGEDIM USER 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

Par Courrier :

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

Par courriel :

igc@cegedim.fr

3. Définitions

Autorité de Certification (AC) : Entité responsable de la génération et de la révocation des Certificats de l'Autorité de Certification ***CEGEDIM USER 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, de l'établissement de la demande de certificat, et le cas échéant, de la conservation de pièces justificatives du Porteur.

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.

Client : Société ou administration cliente de Cegedim qui a contractualisé l'approvisionnement de certificats pour des personnes physiques en relation avec elle.

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 : Désigne la personne physique à qui un Certificat est délivré, sous la responsabilité de l'Autorité d'Enregistrement.

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 v1.2.2 (2018-04) : 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 QUALIFIED CA,*** disponible sur le site Cegedim

[GUIDE] : Guide de Procédure de Révocation Autonome

5. Porteurs des certificats

Les Porteurs de Certificat sont des personnes physiques ayant besoin de signer électroniquement des documents ou de s'authentifier sur un site distant via TLS dans le cadre de leur activité en lien avec le Client.

6. Niveau et usage des certificats

Les Certificats, émis par l'AC ***CEGEDIM USER QUALIFIED CA,*** sont, au sens du règlement eIDAS, des certificats qualifiés de signature électronique sur support qualifié qui permettent aussi l'authentification client TLS. 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 de signature sur support qualifié et d'authentification pour une personne physique	Niveau QCP-n-qscd 0.4.0.194112.1.2	PC : 1.3.6.1.4.1.142057.10.2.1.1.1 CGU : 1.3.6.1.4.1.142057.10.2.1.2.1

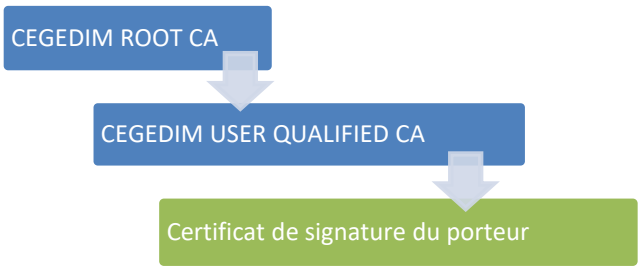
Les Politiques de Certification sont publiées à l'adresse suivante :

http://psco.cegedim.com/CPS

La conformité de la Politique 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 signature d'un Porteur est la suivante :



Les certificats des autorités de certification sont publiées sur :

http://psco.cegedim.com/CRT

8. 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 à laquelle il sera rattaché dans le certificat, ainsi qu'une preuve de son lien avec celle-ci ;

- L'AE vérifie l'authenticité et la validité des documents présentés ;
- Le Porteur accepte les présentes CGU et signe sa demande de certificat ;
- Le Porteur reçoit un dispositif cryptographique matériel dont il choisit le code PIN et sur lequel il génère sa biclé de signature et la requête de certificat ;
- L'Autorité de Certification délivre au porteur un Certificat de signature en réponse à la requête ;
- Le Porteur accepte le Certificat par la signature d'un procès-verbal de réception dont il conserve un exemplaire.

L'AE remet au Porteur un guide pour la révocation en ligne du certificat ([GUIDE]) et les informations nécessaires à la révocation en ligne lui sont soulignées.

Le Certificat de signature du Porteur n'est pas publié, il est inscrit sur son dispositif cryptographique.

9. Modalités de révocation

Le Porteur doit demander sans délai la révocation dans les cas suivants :

- Découverte d'une erreur dans son dossier d'enregistrement ou son Certificat ;
- Usurpation de son identité ou utilisation par un tiers de ses moyens d'authentification ;
- Refus du Certificat ;
- La clé privée est suspectée de compromission, est compromise ou est perdue (perte du dispositif cryptographique) ;
- Le code PIN du dispositif cryptographique est suspectée de compromission, est compromis ou a été perdu.
- Le lien entre le porteur et son entité de rattachement est rompu.

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 par le porteur n'ont pas été respectées ;
- Une rupture technologique nécessite de procéder à la génération de nouvelles biclés.

La révocation d'un Certificat peut être demandée par le Porteur en ligne ou via son AE. En cas de révocation en ligne, le porteur peut se référer au guide qui lui a été remis à la délivrance de son certificat ([GUIDE]). Il est authentifié par des réponses à des questions de sécurité préalablement définies.

10. 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.

11. Limites d'usage

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée à la signature électronique de données ou à l'authentification client TLS.

Tout autre usage est interdit.

12. 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 à l'Autorité d'Enregistrement et l'informer de toute modification éventuelle de celles-ci ;
- Vérifier ses données d'identité dans le demande de Certificat ;

- Générer sa biclé (clé RSA de taille minimale de 2048 bits) dans un dispositif cryptographique qualifié et selon les modalités définies dans la Politique de Certification ;
- 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 choisies ;
- 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 ;
- Informer sans délai son AE de la rupture du lien avec l'entité apparaissant dans 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.

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 ;
- 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 Porteur 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 RGPD) 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. Limite de responsabilité

Cegedim ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des données d'authentification, des Certificats, des CRL.
Cegedim décline sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les Certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné 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 ;
- d'aucun autre dommage.

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.

16. 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.

17. Conditions d'indemnisation

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

18. 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.

19. 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.