

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES - QCP-L

PUBLIC

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

ADMINISTRATION DU DOCUMENT

▪ APPROBATION - VALIDATION

	AUTEUR	APPROBATEUR	CELLULE QUALITE
PRENOM – NOM	STEPHANE GALMICHE	JEAN-MARIE SIMON	ROMAIN VERGNIOL
FONCTION	DIRECTEUR DE PROJETS	DIRECTEUR DE BU	RSI CEGEDIM.CLOUD
DATE	11/05/2021	11/05/2021	11/05/2021

▪ HISTORIQUE DES VERSIONS

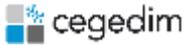
VERSION	DATE	AUTEUR	DESCRIPTIF DES MODIFICATIONS
1.1	03/05/2021	STEPHANE GALMICHE	AJOUT D'UN OID ET PRECISION DES EXIGENCES POUR LES CLES DE CACHET GEREES PAR L'AC CORRECTIONS MINEURES
1.0	15/04/2021	STEPHANE GALMICHE	VERSION INITIALE

Table des matières

1	INTRODUCTION	6
1.1	Présentation générale.....	6
1.2	Identification de la PC.....	6
1.3	Usage des certificats.....	6
1.4	Présentation du service et entités intervenant dans l'IGC.....	7
1.4.1	Autorité de Certification (AC).....	7
1.4.2	Autorité d'Enregistrement (AE).....	7
1.4.3	Porteur de certificats (RCCS).....	8
1.4.4	Utilisateurs de certificats.....	9
2	RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	10
2.1.1	Publication des CRL.....	10
3	IDENTIFICATION ET AUTHENTIFICATION	11
3.1	Nommage	11
3.1.1	Identification du sujet du certificat.....	11
3.1.2	Unicité des noms.....	11
3.1.3	Identification, authentification et rôle des marques déposées.....	11
3.2	Validation initiale de l'identité	11
3.2.1	Méthode pour prouver la possession de la clé privée.....	11
3.2.2	Validation de l'identité d'un organisme.....	11
3.2.3	Validation de l'identité d'un individu.....	12
3.2.4	Informations non vérifiées du porteur.....	12
3.2.5	Validation de l'autorité du demandeur.....	12
3.2.6	Certification croisée d'AC.....	12
3.3	Identification et validation d'une demande de renouvellement	12
3.4	Identification et validation d'une demande de révocation	12
4	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	14
4.1	Demande de certificat	14
4.2	Traitement d'une demande de certificat	14
4.2.1	Exécution des processus d'identification et de validation de la demande.....	14
4.2.2	Acceptation ou rejet de la demande.....	15
4.2.3	Durée d'établissement du certificat.....	15
4.3	Délivrance du certificat	15
4.3.1	Actions de l'AC concernant la délivrance du certificat.....	15
4.3.2	Notification de la délivrance du certificat au porteur.....	15
4.4	Acceptation du certificat	15
4.4.1	Publication du certificat.....	15
4.4.2	Notification aux autres entités de la délivrance du certificat.....	15
4.5	Usages de la bclé et du certificat	15
4.5.1	Utilisation de la clé privée et du certificat par le porteur.....	15
4.5.2	Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	15
4.6	Renouvellement d'un certificat	16

	POLITQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

4.7	Délivrance d'un nouveau certificat suite à changement de la bclé	16
4.8	Modification du certificat	16
4.9	Révocation et suspension des certificats	16
4.9.1	Causes possibles d'une révocation.....	16
4.9.2	Origine d'une demande de révocation	16
4.9.3	Procédure de traitement d'une demande de révocation	17
4.9.4	Délai accordé au porteur pour formuler la demande de révocation	17
4.9.5	Délais de traitement par l'AC d'une demande de révocation	17
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats	17
4.9.7	Fréquence d'établissement des CRL	17
4.9.8	Délai maximum de publication d'une CRL.....	17
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats ..	17
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats	17
4.9.11	Autres moyens disponibles d'information sur les révocations	18
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	18
4.9.13	Suspension de certificats.....	18
4.10	Fonction d'information sur l'état des certificats.....	18
4.10.1	Caractéristiques opérationnelles	18
4.10.2	Disponibilité de la fonction	18
5	MESURES DE SECURITE NON TECHNIQUES	19
6	MESURES DE SECURITE TECHNIQUES.....	20
6.1	Gestion des clés des porteurs	20
6.1.1	Génération des bclés du porteur.....	20
6.1.2	Transmission de la clé privée à son propriétaire.....	20
6.1.3	Transmission de la clé publique à l'AC	20
6.1.4	Taille des clés.....	20
6.1.5	Objectifs d'usage de la clé.....	20
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.....	20
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	20
6.2.2	Séquestre de la clé privée	20
6.2.3	Copie de secours de la clé privée	21
6.2.4	Archivage de la clé privée.....	21
6.2.5	Méthode d'activation de la clé privée.....	21
6.2.6	Méthode de désactivation de la clé privée	21
6.2.7	Méthode de destruction des clés privées	21
6.3	Autres aspects de la gestion des bclés.....	21
6.3.1	Archivage des clés publiques	21
6.3.2	Durées de vie des bclés et des certificats.....	21
6.4	Données d'activation	22
6.4.1	Génération et installation des données d'activation	22
6.4.2	Protection des données d'activation.....	22
7	PROFILS DES CERTIFICATS ET DES CRL	23
7.1	Profil des certificats qualifiés de cachet	23
7.2	Profil du certificat de l'AC CEGEDIM ENTITY QUALIFIED CA.....	23

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

7.3	Profil des CRL	24
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	25
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	26
10	EXIGENCES DE SÉCURITÉ DU DISPOSITIF CRYPTOGRAPHIQUE DU PORTEUR	27
10.1	Exigences sur les objectifs de sécurité	27
10.2	Exigences sur la certification	27

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

1 INTRODUCTION

1.1 Présentation générale

Le présent document, *Politiques et pratiques de certification – AC Cegedim Entités - QCP-I* présente les exigences spécifiques à la politique de certification de l'AC **CEGEDIM ENTITY QUALIFIED CA** de l'IGC de Cegedim.

La présente Politique de Certification (PC) expose les pratiques que l'AC applique et s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. La PC identifie également les obligations et exigences portant sur les autres intervenants et sur les utilisateurs de certificats.

Les mesures de sécurité applicables à l'ensemble des AC de l'IGC Cegedim sont décrites dans le document *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim*.

Les certificats émis dans le cadre de cette PC sont des certificats qualifiés de cachet pour des personnes morales, de niveau QCP-I (selon la norme ETSI 319 411-2), en conformité avec le *Règlement (UE) N° 910/2014 du Parlement européen et du conseil 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*, dit « Règlement eIDAS ».

Ces certificats permettent de réaliser un cachet électronique avancé sur base de certificat qualifié au sens du Règlement eIDAS.

1.2 Identification de la PC

Le présent document intègre les politiques de certification identifiées comme suit :

AC Emettrice	Type de certificat	Niveau eIDAS OID de l'ETSI	OID de la PC
<i>CEGEDIM ENTITY QUALIFIED CA</i>	Certificat qualifié de cachet pour une personne morale qui génère sa clé privée	Niveau QCP-I 0.4.0.194112.1.1	1.3.6.1.4.1.142057.10.3.1.1.1
<i>CEGEDIM ENTITY QUALIFIED CA</i>	Certificat qualifié de cachet pour une personne morale confiant à l'AC la gestion de sa clé privée	Niveau QCP-I 0.4.0.194112.1.1	1.3.6.1.4.1.142057.10.3.3.1.1

La chaîne de certification est la suivante :

- CEGEDIM ROOT CA
 - CEGEDIM ENTITY QUALIFIED CA
 - Certificats finaux de niveau QCP-I

Par commodité, le document est appelé dans la suite du texte « la PC ». Lorsque cela s'avère nécessaire, afin de distinguer les pratiques dépendant de la Politique de Certification du certificat, l'OID de la politique concernée est précisé.

1.3 Usage des certificats

Les restrictions d'utilisation des bclés et des certificats sont définies au chapitre 4.5 ci-dessous.

L'AC utilise une unique bclé pour la signature des certificats et des CRL.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

1.4 Présentation du service et entités intervenant dans l'IGC

1.4.1 Autorité de Certification (AC)

L'Autorité de Certification (AC) définit la politique de certification (PC) et la fait appliquer, garantissant ainsi un certain niveau de confiance aux utilisateurs.

CEGEDIM est la société portant l'autorité de certification **CEGEDIM ENTITY QUALIFIED CA**.

Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de publication des conditions générales d'utilisation, de la PC et des certificats d'AC ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats.

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

L'Autorité de Certification s'engage à respecter la présente Politique de Certification et les réglementations en vigueur, en particulier :

- 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'AC demande la révocation du Certificat Porteur dès qu'un événement anormal, précisé au 4.9.1, a été constaté ;
- L'AC conserve les informations qui pourraient s'avérer nécessaires à titre de preuve de bon fonctionnement de son service et d'intégrité des données utilisées ;
- L'AC respecte la protection des données à caractère personnel (en particulier le règlement RGPD) dans l'ensemble de ses activités.

L'Autorité de Certification peut être contactée :

- Par courrier :

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

- Par courriel :

igc@cegedim.fr

1.4.2 Autorité d'Enregistrement (AE)

L'Autorité d'Enregistrement a en charge les fonctions suivantes conformément aux règles définies par l'AC :

- La vérification des informations du RCCS et du service applicatif, ainsi que de leur entité de rattachement afin de garantir la validité des informations contenues dans le certificat ;
- La constitution du dossier d'enregistrement suite aux vérifications ci-dessus ;
- La transmission de la demande de certificat à l'AC ;
- L'archivage des dossiers d'enregistrement de certificat ;
- La vérification des demandes de révocation de certificat.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

Les fonctions de vérification des informations du porteur, de constitution puis d'archivage du dossier sont assurées soit directement par Cegedim, soit par une entité cliente de Cegedim. La vérification des demandes de révocation est toujours réalisée par l'AE.

L'Autorité d'Enregistrement s'engage à respecter la présente Politique de Certification et les réglementations en vigueur, en particulier :

- L'AE vérifie avec attention les données d'identité du Porteur ;
- L'AE demande la révocation du Certificat Porteur dès qu'un événement anormal, précisé au 4.9.1, a été constaté ;
- L'AE conserve 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 respecte la protection des données à caractère personnel (en particulier le règlement RGPD) dans l'ensemble de ses activités.

1.4.3 Porteur de certificats (RCCS)

Les certificats cachet serveur sont délivrés à des entités ou à des services applicatifs d'une entité, qui sont le sujet des certificats. Un certificat cachet serveur est placé sous la responsabilité d'une personne physique, le responsable du certificat cachet serveur (RCCS). Dans le cadre de cette PC, le RCCS est désigné comme le porteur du certificat.

En cas d'interruption des fonctions du RCCS, l'entité doit lui nommer un successeur et en informer l'AC.

La fiabilité du cachet électronique et du certificat 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 les données d'identité dans la demande de Certificat ;
- Garantir la confidentialité du secret associé et des réponses aux questions de sécurité qu'il a choisies ;
- Respecter 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 de la présente Politique de Certification et des CGU associées.

Selon le cas, les obligations suivantes s'appliquent aussi :

- [Niveau QCP-I avec clé privée générée par le porteur](#) :
 - o 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 ;
 - o Assurer la sécurité et le contrôle exclusif de son dispositif cryptographique ;
- [Niveau QCP-I avec clé privée gérée par l'AC](#) :
 - o 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 ;
 - o 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 ;

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

- Assurer la sécurité du ou des moyens d'authentification utilisés ainsi que de leur données d'activation.

1.4.4 Utilisateurs de certificats

L'utilisateur de certificat est l'entité ou la personne physique qui utilise un certificat et qui s'y fie pour vérifier un cachet réalisé avec le certificat émis selon cette PC.

Les utilisateurs de certificats doivent respecter l'usage des certificats prévu dans cette PC, les contraintes d'utilisation détaillées au §4.9.6 et prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

Voir *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim*.

2.1.1 Publication des CRL

L'AC publie la liste des certificats révoqués (CRL) aux adresses suivantes :

<http://psco.cegedim.com/CRL/CEGEDIMENTITYQUALIFIEDCA.crl>

	POLITIQUE ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Identification du sujet du certificat

Les noms choisis pour désigner le sujet des certificats sont explicites.

L'entité (et optionnellement le service) est identifiée dans le champ « Objet » (« *Subject* » en anglais) du certificat par les champs suivants de la norme ETSI EN 319 412 :

COMMON NAME	Nom d'un service (optionnel) et nom de l'entité à laquelle est affecté le certificat (obligatoire)
SERIAL NUMBER	Numéro unique de la demande de certificat
ORGANIZATION IDENTIFIER	Identifiant unique normalisé de l'entité selon la norme EN 319 412-1. Pour une entité immatriculée en France, cet identifiant est de la forme NTRFR-SIREN
ORGANIZATION	Dénomination sociale de l'entité telle qu'elle est indiquée sur les justificatifs d'identité présentés à l'enregistrement
COUNTRY	Code ISO 3166-1 sur 2 lettres du pays d'immatriculation de l'entité

Les certificats de test sont clairement identifiés par le préfixe « TEST » placé en début du champ CN, (c'est-à-dire devant le nom du service).

3.1.2 Unicité des noms

Le DN du champ « *subject* » de chaque certificat permet d'identifier de façon unique celui-ci au sein du domaine de l'AC, grâce au code du pays, à l'identifiant de l'organisation et le cas échéant au nom du service.

L'AC est garante de l'unicité des noms des porteurs.

3.1.3 Identification, authentification et rôle des marques déposées

Les informations utilisées dans les certificats sont celles indiquées dans la demande et vérifiées par l'Autorité d'Enregistrement.

L'AC s'efforce de résoudre à l'amiable tout litige portant sur la revendication d'utilisation d'un nom.

3.2 Validation initiale de l'identité

La vérification de l'identité des porteurs est du ressort de l'AE ; elle est réalisée conformément aux 3.2.3 et 3.2.5 ci-dessous.

3.2.1 Méthode pour prouver la possession de la clé privée

[Niveau QCP-I avec clé privée générée par le porteur](#)

Le RCCS fournit à l'AE une preuve de possession de la clé privée sous la forme d'une CSR, contenant la clé publique et signée par la clé privée.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Sans objet, la privée est générée puis gérée par l'AC.

3.2.2 Validation de l'identité d'un organisme

Voir 3.2.5.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

3.2.3 Validation de l'identité d'un individu

Le porteur (RCCS) fournit au minimum les informations suivantes à l'AE :

- Son nom et son prénom tels qu'ils apparaissent sur ses documents d'identité ;
- Une adresse courriel à laquelle l'AC peut le joindre.

Il appartient à l'AE de valider l'exactitude de l'identité de la personne (nom, prénom) par l'examen d'une pièce d'identité présentée en face à face (présence physique du RCCS). Les pièces d'identité acceptées sont les titres authentiques en cours de validité parmi les suivants :

- Carte nationale d'identité ;
- Passeport ;
- Carte de séjour.

3.2.4 Informations non vérifiées du porteur

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Il appartient à l'AE de valider l'autorité du RCCS par l'examen de :

- Pour une entreprise, toute pièce valide lors de la demande de certificat (extrait Kbis ou certificat d'identification au répertoire national des entreprises et de leurs établissements ou inscription au répertoire des métiers...) attestant de l'existence de l'entreprise et portant le numéro SIREN de celle-ci ou, à défaut, une autre pièce attestant l'identification unique de l'entreprise qui figurera dans le certificat ;
- Pour une administration, toute pièce valide lors de la demande de certificat, portant délégation ou subdélégation de l'autorité responsable de la structure administrative ;
- Une habilitation du RCCS à demander des certificats pour le compte de l'entité, signée par le représentant légal ou une personne autorisée.

3.2.6 Certification croisée d'AC

Pas d'exigence en l'état actuel de la politique.

3.3 Identification et validation d'une demande de renouvellement

Le renouvellement d'un certificat peut être demandé par le RCCS 3 mois avant l'expiration du certificat concerné.

Le renouvellement est réalisé en suivant la procédure de demande initiale.

3.4 Identification et validation d'une demande de révocation

La révocation d'un certificat peut être demandé par le RCCS ou le responsable légal de l'entité pour laquelle est établie le certificat.

La demande doit être réalisée par courrier papier ou électronique, et comporter :

- Le nom et le prénom du demandeur de la révocation ;
- L'adresse courriel du demandeur ;
- Une copie de la pièce d'identité du demandeur ;
- L'identification du certificat à révoquer :
 - o Le nom du service et de l'entité tels qu'ils apparaissent dans le certificat ;

	POLITIKES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

- Les dates de validité du certificat.
- La signature du demandeur

La demande doit être transmise à l'AE en utilisant l'adresse de contact précisée dans les Conditions Générales d'Utilisation du certificat.

L'AE vérifie les éléments de la demande et l'identité du demandeur en le contactant grâce aux informations recueillies au moment de la demande du certificat (téléphone, email...).

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

Toute demande du certificat est déposée directement auprès d'une Autorité d'Enregistrement par le (futur) RCCS.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

Le processus de demande est le suivant :

1. Le RCCS se présente en face à face à l'AE avec une pièce d'identité ;
2. L'AE vérifie l'identité du RCCS ;
3. L'AE vérifie l'identité de l'entité par le contrôle d'une preuve d'existence légale de l'entité portant son numéro d'identification ;
4. Si le RCCS n'est pas le représentant légal de l'entité, l'AE vérifie l'habilitation du RCCS pour réaliser cette demande de certificat par le contrôle d'un document signé électroniquement par le Responsable Légal ou une personne autorisée de l'entité pour laquelle est établie le certificat.
5. L'AE établit le formulaire de demande en reportant au minimum :
 - a. Le nom (raison sociale par exemple) de l'entité et optionnellement le nom du service pour lequel le certificat est établi ;
 - b. Le numéro d'identification de l'entité et ses coordonnées postales ;
 - c. Le nom et prénom et l'adresse de courriel du RCCS ;
 - d. Le nom et prénom et l'adresse de courriel du signataire de l'habilitation du RCCS.
6. L'AE présente le formulaire de demande au RCCS et lui demande de vérifier l'exactitude de ces informations ;
7. L'AE présente les CGU au RCCS et lui demande de les accepter ;
8. Le RCCS signe électroniquement le formulaire de demande et les CGU ;
9. Enregistrement de la CSR :
 - a. Niveau QCP-I avec clé privée générée par le porteur : Le RCCS fournit à l'AE la requête de certificat (CSR) qu'il a générée au préalable sur un matériel cryptographique conforme aux exigences de l'AC ;
 - b. Niveau QCP-I avec clé privée gérée par l'AC : L'opérateur AE demande à l'AC de générer une bi-clé et la CSR associée pour le compte du porteur ;
10. L'AE archive le dossier d'enregistrement comprenant :
 - a. Le formulaire de demande signé par le RCCS ;
 - b. Les CGU signées par le RCCS ;
 - c. La copie de la preuve d'existence légale de l'entité ;
 - d. La copie de la pièce d'identité du RCCS ;
 - e. L'habilitation du RCCS.
11. L'AE transmet la demande et la CSR à l'AC.

	POLITIQUE ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Pour ce cas, le RCCS indique à l'opérateur AE le mode d'authentification qui sera utilisé pour l'activation de la clé de cachet. Il fournira les informations nécessaires à la vérification de cette authentification.

4.2.2 Acceptation ou rejet de la demande

La demande peut être acceptée ou rejetée par l'AE lors du traitement de la demande. La demande peut aussi être rejetée par l'AC si le contenu de la CSR ne convient pas.

Tout refus est dûment justifié et notifié au RCCS par l'AE.

4.2.3 Durée d'établissement du certificat

Le certificat est émis immédiatement après l'acceptation de la demande.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

L'AC vérifie l'origine et l'intégrité de la demande reçue de l'AE. L'AC déclenche alors le processus de génération du certificat destiné au RCCS.

Le certificat complet et exact est remis en main propre à son porteur par l'opérateur AE sur un support amovible de stockage.

4.3.2 Notification de la délivrance du certificat au porteur

Sans objet.

4.4 Acceptation du certificat

Le porteur accepte le certificat par la signature d'un procès-verbal de réception lors de la remise du certificat par l'opérateur de l'AE.

4.4.1 Publication du certificat

Les certificats émis ne font pas l'objet d'une publication.

4.4.2 Notification aux autres entités de la délivrance du certificat

L'AE est informée de la génération du certificat, et est chargée de le transmettre au RCCS.

4.5 Usages de la clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le porteur

L'utilisation des clés privées est limitée au scellement de données.

Cet usage est indiqué dans les extensions des certificats.

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

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. Ils doivent vérifier la révocation ou l'expiration des certificats en analysant le contenu de ces certificats et la liste de révocation mise à disposition par l'AC.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

4.6 Renouvellement d'un certificat

Le renouvellement d'un certificat au sens du RFC 3647 (sans changement de bclé) n'est pas autorisé par cette PC.

4.7 Délivrance d'un nouveau certificat suite à changement de la bclé

Le renouvellement est compris, dans le cadre de cette PC, comme la délivrance d'un nouveau certificat pour le même sujet mais basé sur une nouvelle bclé.

Le renouvellement est réalisé en suivant la procédure de demande initiale

4.8 Modification du certificat

La modification du certificat n'est pas autorisée par cette PC .

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- Les modalités d'utilisation du certificat n'ont pas été respectées ;
- Le porteur n'a pas respecté ses obligations découlant de la PC de l'AC ou des CGU correspondantes ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ou dans le certificat ;
- Le porteur refuse son certificat ;
- L'entité a interrompu son service de cachet ;
- La clé privée du porteur est suspectée de compromission, est compromise ou est perdue (éventuellement les données d'activation associées ou bien les secrets d'authentification utilisés dans la cas d'une clé de cachet gérée par l'AC) ;
- Révocation de l'AC ;
- Rupture technologique, nécessitant de procéder à la génération de nouvelles bclés (longueurs des clés trop faibles, algorithmes de hachage compromis).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

La fin de contrat entre Cegedim et le client ayant commandé les certificats n'entraîne pas la révocation des dits certificats.

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander la révocation d'un certificat sont :

- Le RCCS ;
- Le représentant légal de l'entité apparaissant dans le certificat ;
- L'AE ;
- L'AC.

	POLITIQUE ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

4.9.3 Procédure de traitement d'une demande de révocation

Les exigences d'identification et de validation effectuée par la fonction de gestion des révocations sont décrites au 3.4.

Les informations suivantes doivent figurer dans la demande de révocation de certificat :

- Le nom du service et de l'entité tels qu'ils apparaissent dans le certificat ;
- Le nom et le prénom du RCCS ou du représentant légal ;
- L'adresse courriel du RCCS ou du représentant légal, telle qu'indiquée à son enregistrement.

Si le RCCS ou le représentant légal n'a pas accès à cette adresse de courriel, il contacte l'AC (directement ou par l'intermédiaire de son AE).

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation sera diffusée via une CRL signée.

Le demandeur de la révocation sera informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le porteur du certificat n'est pas le demandeur, il sera également informé de la révocation effective de son certificat.

Niveau QCP-I avec clé privée gérée par l'AC

Dans le cas où la clé privée du porteur est gérée par l'AC, l'AC procède après révocation à la destruction de la clé privée (et de toutes ses copies) correspondant au certificat révoqué.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le RCCS ou une personne autorisée a connaissance qu'une des causes possibles de révocation est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délais de traitement par l'AC d'une demande de révocation

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur à 24h. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'utilisateur d'un certificat de porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

4.9.7 Fréquence d'établissement des CRL

Les CRL sont publiées quotidiennement.

4.9.8 Délai maximum de publication d'une CRL

La publication des CRL est de maximum 30 minutes après leur établissement.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Sans objet (le protocole OCSP n'est pas implémenté).

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Seule la vérification par les CRL est disponible (cf. chapitre 4.9.6 ci-dessus).

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Le porteur s'engage, au travers l'acceptation des CGU, à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé en cas de compromission de la clé privée du porteur et après avoir été informé de la compromission de la clé privée de l'AC ayant émis son certificat.

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fera l'objet d'une information clairement diffusée sur le site Internet de l'AC.

4.9.13 Suspension de certificats

La suspension de certificats n'est pas autorisée dans la présente PC.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de CRL. Ces CRL sont au format V2.

La CRL est accessible à l'adresse donnée au §2.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24 et 7 jours sur 7.

Les systèmes de publication des CRL ont un taux de disponibilité de 99,5 pour cent, et respectent une durée maximum d'indisponibilité de 4 heures.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

5 MESURES DE SECURITE NON TECHNIQUES

Se référer au document *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim*.

	POLITIKES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

6 MESURES DE SECURITE TECHNIQUES

Se référer au document *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim* pour toutes les mesures transverses aux différentes AC. Le présent chapitre ne traite que des mesures spécifiques à l'AC « CEGEDIM ENTITY QUALIFIED CA ».

6.1 Gestion des clés des porteurs

6.1.1 Génération des biclés du porteur

[Niveau QCP-I avec clé privée générée par le porteur](#)

Les clés des porteurs sont générées sous le contrôle du porteur sur un dispositif répondant aux exigences du §10.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Les clés des porteurs sont générées par l'AC sur un dispositif répondant aux exigences du §10.

6.1.2 Transmission de la clé privée à son propriétaire

[Niveau QCP-I avec clé privée générée par le porteur](#)

Sans objet, la clé privée est générée directement sur le dispositif cryptographique du porteur.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

La clé privée n'est pas transmise à son propriétaire, elle reste sous la protection exclusive de l'AC.

6.1.3 Transmission de la clé publique à l'AC

[Niveau QCP-I avec clé privée générée par le porteur](#)

La transmission de la clé publique du porteur à l'AC est protégée en intégrité et en authenticité dans une CSR.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

La clé publique est générée et protégée sur un dispositif cryptographique de l'AC, et protégée en intégrité et en authenticité dans une CSR pour l'établissement du certificat.

6.1.4 Taille des clés

Les biclés des porteurs sont des clés RSA de taille minimale de 4096 bits.

6.1.5 Objectifs d'usage de la clé

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée aux services de cachet.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

Voir §10.

6.2.2 Séquestre de la clé privée

Les clés privées des porteurs ne sont en aucun cas séquestrées.

	POLITIQUE ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

6.2.3 Copie de secours de la clé privée

[Niveau QCP-I avec clé privée générée par le porteur](#)

Les clés privées des porteurs ne font l'objet d'aucune copie de secours par l'AC.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Les clés privées des porteurs peuvent faire l'objet de copie de redondance ou de secours afin de garantir au porteur une meilleure disponibilité de sa clé. Ces copies sont créées, conservées et détruites dans des conditions satisfaisant en toutes circonstances les exigences du §10.

6.2.4 Archivage de la clé privée

Les clés privées des porteurs ne sont pas archivées, ni par l'AC, ni par aucune des composantes de l'IGC.

6.2.5 Méthode d'activation de la clé privée

[Niveau QCP-I avec clé privée générée par le porteur](#)

L'activation de la clé privée du porteur est contrôlée via des données d'activation qui lui sont propres et permet de répondre aux exigences définies au §10.1.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

L'activation de la clé privée du porteur est subordonnée à une authentification forte et dynamique d'un système ou d'un personnel de l'entité cliente selon les modalités définies par le porteur (le RCCS) auprès de l'AC.

6.2.6 Méthode de désactivation de la clé privée

[Niveau QCP-I avec clé privée générée par le porteur](#)

Le porteur met en œuvre les conditions de désactivation de la clé privée permettent de répondre aux exigences définies au §10.1.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

La clé privée du porteur est désactivée en fin de session authentifiée du porteur auprès de l'AC.

6.2.7 Méthode de destruction des clés privées

[Niveau QCP-I avec clé privée générée par le porteur](#)

Le porteur est l'unique détenteur de sa clé privée. En fin de vie, il est responsable de la destruction de sa clé de manière logique ou physique.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

La clé privée du porteur est détruite, ainsi que toutes ses copies, par l'AC, après expiration ou révocation du certificat, selon les mécanismes sécurisés du dispositif cryptographique qui la contient.

6.3 Autres aspects de la gestion des biclés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durées de vie des biclés et des certificats

Les biclés et les certificats des porteurs couverts par la présente ont la même durée de vie.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

[Niveau QCP-I avec clé privée générée par le porteur](#)

Le porteur génère lui-même ses données d'activation en cohérence avec les exigences du §10 applicables à son dispositif cryptographique.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Le porteur est responsable de la génération et de l'installation des données d'activation en respectant les exigences de sécurité associées au moyen d'authentification convenu avec l'AC.

6.4.2 Protection des données d'activation

[Niveau QCP-I avec clé privée générée par le porteur](#)

Le porteur est responsable de la protection de ses données d'activation dans le respect des exigences du §10 applicables à son dispositif cryptographique.

[Niveau QCP-I avec clé privée gérée par l'AC](#)

Le porteur est responsable de la protection des données d'activation dans le respect des exigences de sécurité associées au moyen d'authentification convenu avec l'AC.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

7 PROFILS DES CERTIFICATS ET DES CRL

7.1 Profil des certificats qualifiés de cachet

Les certificats qualifiés de cachet de niveau QCP-I émis pour les porteurs finaux ont le gabarit suivant :

Champs de base		Valeur du champ
Version		2 (version 3)
Numéro de série		Numéro unique sur 16 octets
Sujet		CN = <Service (optionnel) - > <Nom de l'entité> SERIALNUMBER = <Numéro unique de demande de certificat> OI = <identifiant normalisé de l'entité> O = <Nom de l'entité> C = <Code de pays d'immatriculation de l'entité>
Emetteur		CN = CEGEDIM ENTITY QUALIFIED CA OI = NTRFR-350422622 O = CEGEDIM C = FR
Durée de validité		3 ans
Algorithme de clé publique		RSA
Longueur des clefs		4096 bits
Algorithme de signature		SHA512WithRSA
Extensions		Criticité
Basic Constraints	N	CA : Faux
Key Usage	O	Non Repudiation et DigitalSignature
Certificate Policies	N	1. PolicyIdentifier : Cas de la clé privée générée par le porteur 1.3.6.1.4.1.142057.10.3.1.1.1 Cas de la clé privée gérée par l'AC 1.3.6.1.4.1.142057.10.3.3.1.1 Qualifier : CPS = http://psco.cegedim.com 2. PolicyIdentifier : 0.4.0. 194112.1.1
Authority Key Identifier	N	Hash SHA-1 de la clé publique du certificat de l'AC
Subject Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat
Authority Information Access	N	accessMethod : id-ad-calssuers accessLocation : http://psco.cegedim.com/CRT/CEGEDIMENTITYQUALIFIEDCA.crt
CRL Distribution Points	N	URI de téléchargement de la CRL de l'AC : http://psco.cegedim.com/CRL/CEGEDIMENTITYQUALIFIEDCA.crl
qcStatements	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-6 = id-etsi-qct-eseal

7.2 Profil du certificat de l'AC CEGEDIM ENTITY QUALIFIED CA

Le certificat de l'Autorité de Certification CEGEDIM ENTITY QUALIFIED CA a le gabarit suivant :

Champs de base		Valeur du champ
Version		2 (version 3)
Numéro de série		Numéro unique sur 16 octets
Sujet		CN = CEGEDIM ENTITY QUALIFIED CA OI = NTRFR-350422622

PUBLIC

	POLITIQUE ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

	O = CEGEDIM C = FR	
Emetteur	CN = CEGEDIM ROOT CA OI = NTRFR-350422622 O = CEGEDIM C = FR	
Durée de validité	10 ans	
Algorithme de clé publique	RSA	
Longueur des clefs	4096 bits	
Algorithme de signature	SHA512WithRSA	
Extensions	Criticité	Valeur de l'extension
Basic Constraints	O	CA : Vrai Longueur de chemin : 0
Key Usage	O	keyCertSign crlSign
Certificate Policies	N	PolicyIdentifier : AnyPolicy (2.5.29.32.0)
Authority Key Identifier	N	Hash SHA-1 de la clé publique de l'AC Racine
Subject Key Identifier	N	Hash SHA-1 de la clé publique de ce certificat
Authority Information Access	N	accessMethod : id-ad-calssuers accessLocation : http://psco.cegedim.com/CRT/CEGEDIMROOTCA.crt
CRL Distribution Points	N	URI de l'ARL de l'AC Racine : http://psco.cegedim.com/CRL/CEGEDIMROOTCA.crl

7.3 Profil des CRL

Les CRL émises par l'Autorité de Certification CEGEDIM ENTITY QUALIFIED CA ont le gabarit suivant :

Champs de base	Valeur du champ	
Version	1 (version 2)	
Emetteur	CN = CEGEDIM ENTITY QUALIFIED CA OI = NTRFR-350422622 O = CEGEDIM C = FR	
This Update	Date de génération de la CRL	
Next Update	6 jours après la date de génération	
Algorithme de signature	SHA512WithRSA	
Liste	Valeur du champ	
Revoked Certificates	Serial Number : Numéro de série du certificat révoqué Revocation Date : Date de révocation	
Extensions	Criticité	Valeur de l'extension
Authority Key Identifier	N	Hash SHA-1 de la clé publique de l'AC
CRL Number	N	Numéro séquentiel de la liste
ExpiredCertOnCRL	N	Date d'émission de la première CRL (les certificats révoqués ne sont jamais retirés de la CRL)

PUBLIC

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Se référer au document *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim*.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

Se référer au document *Politiques et pratiques de certification – Mesures de sécurité communes aux AC Cegedim*.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM ENTITES QCP-L	
V 1.1		

10 EXIGENCES DE SÉCURITÉ DU DISPOSITIF CRYPTOGRAPHIQUE DU PORTEUR

10.1 Exigences sur les objectifs de sécurité

Le dispositif cryptographique utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et générer sa biclé doit répondre aux exigences de sécurité suivantes :

- Garantir que la génération de la biclé est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la biclé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Être en mesure de générer une authentification ou une signature qui ne peuvent être falsifiées sans la connaissance de la clé privée ;
- Protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

10.2 Exigences sur la certification

Le dispositif cryptographique du porteur doit être certifié *Critères Communs* au niveau EAL 4 ou supérieur, ou à des critères d'évaluation équivalents reconnus à l'échelle nationale ou internationale en matière de sécurité des technologies de l'information, selon un profil de protection répondant aux exigences ci-dessus (10.1), sur la base d'une analyse des risques et tenant compte des mesures physiques et non techniques de sécurité.