



	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES - LCP ET NCP

PUBLIC

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

ADMINISTRATION DU DOCUMENT

- APPROBATION

	AUTEUR	APPROBATEUR
PRENOM – NOM	STEPHANE GALMICHE	HONG GIRAULT
FONCTION	DIRECTEUR DE PROJETS	DIRECTEUR D'ACTIVITE
DATE	01/06/2023	15/06/2023

- HISTORIQUE DES VERSIONS

VERSION	DATE	AUTEUR	DESCRIPTIF DES MODIFICATIONS
1.4	01/06/2023	STEPHANE GALMICHE	SUPPRESSION DE LA POSSIBILITE DE REVOQUER
1.3	17/05/2023	STEPHANE GALMICHE	ENVOI DU CODE A USAGE UNIQUE POSSIBLE PAR COURRIEL SUPPRESSION DE L'AED
1.2	04/06/2021	STEPHANE GALMICHE	INDICATION DU RECOURS A UN SERVICE EXTERNE D'ANALYSE DES PIECES D'IDENTITE POUR LE NIVEAU LCP
1.1	03/05/2021	STEPHANE GALMICHE	AJOUT DE L'EXTENSION SUBJECT ALTERNATIVE NAME & CORRECTIONS MINEURES
1.0	15/04/2021	STEPHANE GALMICHE	VERSION INITIALE

PUBLIC



	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

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.....	8
1.4.4	Utilisateurs de certificats.....	8
2	RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	9
2.1.1	Publication des CRL.....	9
3	IDENTIFICATION ET AUTHENTIFICATION	10
3.1	Nommage	10
3.1.1	Unicité des noms.....	10
3.1.2	Identification, authentification et rôle des marques déposées.....	10
3.2	Validation initiale de l'identité	10
3.2.1	Méthode pour prouver la possession de la clé privée.....	10
3.2.2	Validation de l'identité d'un organisme.....	10
3.2.3	Validation de l'identité d'un individu.....	10
3.2.4	Informations non vérifiées du porteur.....	11
3.2.5	Validation de l'autorité du demandeur.....	11
3.2.6	Certification croisée d'AC.....	11
3.3	Identification et validation d'une demande de renouvellement	11
3.4	Identification et validation d'une demande de révocation	11
4	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	12
4.1	Demande de certificat	12
4.1.1	Origine d'une demande de certificat.....	12
4.1.2	Processus et responsabilités pour l'établissement d'une demande de certificat.....	12
4.2	Traitement d'une demande de certificat	12
4.2.1	Exécution des processus d'identification et de validation de la demande.....	12
4.2.2	Acceptation ou rejet de la demande.....	13
4.2.3	Durée d'établissement du certificat.....	13
4.3	Délivrance du certificat	13
4.3.1	Actions de l'AC concernant la délivrance du certificat.....	13
4.3.2	Notification de la délivrance du certificat au porteur.....	13
4.4	Acceptation du certificat	13
4.4.1	Publication du certificat.....	13
4.4.2	Notification aux autres entités de la délivrance du certificat.....	13
4.5	Usages de la bicyclette et du certificat	13
4.5.1	Utilisation de la clé privée et du certificat par le porteur.....	13
4.5.2	Utilisation de la clé publique et du certificat par l'utilisateur du certificat.....	14

PUBLIC

4.6	Renouvellement d'un certificat	14
4.7	Délivrance d'un nouveau certificat suite à changement de la biclé	14
4.8	Modification du certificat	14
4.9	Révocation et suspension des certificats	14
4.9.1	Causes possibles d'une révocation.....	14
4.9.2	Origine d'une demande de révocation	14
4.9.3	Procédure de traitement d'une demande de révocation	14
4.9.4	Délai accordé au porteur pour formuler la demande de révocation	14
4.9.5	Délais de traitement par l'AC d'une demande de révocation	14
4.9.6	Exigences de vérification de la révocation par les utilisateurs de certificats	14
4.9.7	Fréquence d'établissement des CRL	14
4.9.8	Délai maximum de publication d'une CRL.....	15
4.9.9	Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats ..	15
4.9.10	Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 15	15
4.9.11	Autres moyens disponibles d'information sur les révocations	15
4.9.12	Exigences spécifiques en cas de compromission de la clé privée	15
4.9.13	Suspension de certificats.....	15
4.10	Fonction d'information sur l'état des certificats.....	15
4.10.1	Caractéristiques opérationnelles	15
4.10.2	Disponibilité de la fonction	15
5	MESURES DE SECURITE NON TECHNIQUES	16
6	MESURES DE SECURITE TECHNIQUES.....	17
6.1	Gestion des clés des porteurs	17
6.1.1	Génération des bi-clés du porteur	17
6.1.2	Transmission de la clé privée à son propriétaire.....	17
6.1.3	Transmission de la clé publique à l'AC	17
6.1.4	Taille des clés.....	17
6.1.5	Objectifs d'usage de la clé.....	17
6.2	Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques.....	17
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	17
6.2.2	Séquestre de la clé privée	17
6.2.3	Copie de secours de la clé privée	17
6.2.4	Archivage de la clé privée.....	17
6.2.5	Méthode d'activation de la clé privée.....	17
6.2.6	Méthode de désactivation de la clé privée	17
6.2.7	Méthode de destruction des clés privées	18
6.3	Autres aspects de la gestion des bi-clés	18
6.3.1	Archivage des clés publiques	18
6.3.2	Durées de vie des bi-clés et des certificats	18
6.4	Données d'activation	18
6.4.1	Génération et installation des données d'activation	18
6.4.2	Protection des données d'activation.....	18
7	PROFILS DES CERTIFICATS ET DES CRL	19
7.1	Profil des certificats des porteurs pour le niveau NCP.....	19

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

7.2	Profil des certificats des porteurs pour le niveau LCP	19
7.3	Profil du certificat de CEGEDIM USER ADVANCED CA	20
7.4	Profil des CRL de CEGEDIM USER ADVANCED CA	21
8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	22
9	AUTRES PROBLEMATIQUES METIERS ET LEGALES	23

1 INTRODUCTION

1.1 Présentation générale

Le présent document, *Politiques et pratiques de certification – AC Cegedim Personnes Physiques - LCP et NCP* présente les exigences spécifiques aux politiques de certification de l'AC **CEGEDIM USER ADVANCED 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 des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim*.

Les Certificats émis dans le cadre de cette PC sont des certificats de signature pour des personnes physiques, de niveau LCP ou NCP (selon la norme ETSI 319 411-1), 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 une signature électronique avancée à la volée 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 USER ADVANCED CA</i>	Certificat de signature pour une personne physique enregistrée en face à face Usage interne Cegedim	Niveau NCP 0.4.0.2042.1.1	1.3.6.1.4.1.142057.10.4.1.1.1
<i>CEGEDIM USER ADVANCED CA</i>	Certificat de signature pour une personne physique enregistrée en ligne	Niveau LCP 0.4.0.2042.1.3	1.3.6.1.4.1.142057.10.4.2.1.1

La chaîne de certification est la suivante :


- CEGEDIM ROOT CA
 - CEGEDIM USER ADVANCED CA
 - Certificats finaux de niveau NCP et LCP

Par commodité, le document est appelé dans la suite du texte « la PC ». Lorsque cela s'avère nécessaire, afin de distinguer les pratiques dépendant du niveau de sécurité du certificat, le niveau du certificat concerné est précisé.

Les certificats de niveau NCP (OID : 1.3.6.1.4.1.142057.10.4.1.1.1) ne sont délivrés qu'à des collaborateurs Cegedim pour un usage interne.

1.3 Usage des certificats

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

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

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

1.4 Présentation du service et entités intervenant dans l'IGC

1.4.1 Autorité de Certification (AC)

L'Autorité de Certification (AC) définit les politiques de certification (PC) et les fait appliquer, garantissant ainsi un niveau de confiance défini aux utilisateurs.

Cegedim est la société portant l'autorité de certification **CEGEDIM USER ADVANCED CA**.

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

- Fonctions d'enregistrement ;
- 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 l'entière 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 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 des demandeurs de certificat, afin de garantir la validité des informations contenues dans le certificat ;
- La constitution du dossier d'enregistrement et de demande suite aux vérifications ci-dessus ;
- L'archivage des dossiers d'enregistrement et de demande de certificat.

L'AE expose un service d'enregistrement en ligne intégré à l'outil de signature Cegedim.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

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 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.

Niveau LCP

L'AE utilise un service externe (fourni par un prestataire de Cegedim) d'analyse de la copie de la pièce d'identité du porteur pour décider de valider ou non son identité. L'AE conserve l'entière responsabilité de cette décision.

1.4.3 Porteur de certificats

Les porteurs de certificats sont des personnes physiques qui demandent un certificat de signature pour elles-mêmes, dans le cadre d'une cérémonie de signature.


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 ;
- Vérifier ses données d'identité dans la demande de Certificat ;
- Accepter que le moteur de signature Cegedim génère, utilise puis détruit la clé privée en son nom et selon les modalités définies dans la Politique de Certification (clé RSA de taille minimale de 2048 bits) ;
- Assurer la sécurité et le contrôle exclusif du compte de messagerie ou du téléphone mobile sur lequel il reçoit le code d'authentification à usage unique ;
- Accepter la conservation par l'AE et l'AC du dossier d'enregistrement et des journaux d'événements relatifs à son Certificat, afin de les produire comme preuve, le cas échéant en justice ;
- Respecter, plus largement, les obligations qui lui incombent dans le cadre des présentes CGU et de la Politique de Certification associée.

1.4.4 Utilisateurs de certificats

Les utilisateurs de certificat sont les entités ou les personnes physiques qui utilisent un certificat et qui s'y fient pour vérifier une signature électronique provenant du porteur du certificat.

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 PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		


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

Voir Politiques et pratiques des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim.

2.1.1 Publication des CRL

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

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

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

Les noms choisis pour désigner les porteurs sont explicites, par la précision de leur nom, prénom et adresse de messagerie.

Le porteur est identifié dans le champ « Objet » (« *Subject* » en anglais) du certificat par les champs suivants de la norme ETSI EN 319 412 :

EMAIL	Adresse de messagerie du porteur
COMMON NAME	Nom convivial du porteur, constitué du prénom et du nom du porteur
GIVEN NAME	Prénom du porteur
SURNAME	Nom du porteur
SERIAL NUMBER	Identifiant unique affecté au porteur pour une cérémonie de signature
COUNTRY	FR Code ISO 3166-1 sur 2 lettres du pays d'immatriculation de Cegedim

Les certificats de test sont clairement identifiés par le préfixe ou le suffixe « TEST » placé dans le champ CN.

3.1.1 Unicité des noms

L'AC est garante de l'unicité des champs Distinguished Name des certificats qu'elle émet. Pour cela, le champ « Objet » de chaque certificat intègre le nom, le prénom et un identifiant unique du porteur distinct pour chaque cérémonie de signature.

3.1.2 Identification, authentification et rôle des marques déposées

Sans objet, les certificats sont émis pour des personnes physiques.

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

La requête de certificat est signée avec la clé privée associée à la clé publique.


3.2.2 Validation de l'identité d'un organisme

Sans objet, le certificat est émis pour une personne physique sans porter de lien avec une personne morale.

3.2.3 Validation de l'identité d'un individu

L'AE valide l'exactitude de l'identité du porteur (nom, prénom) par l'examen d'une pièce d'identité présentée par celui-ci. Les pièces d'identité acceptées sont les titres authentiques en cours de validité parmi les suivants :

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

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

Niveau NCP

L'opérateur d'enregistrement de l'AE vérifie l'identité du porteur par rapport à sa pièce d'identité lors d'un face à face.

Niveau LCP

L'AE vérifie la copie de la pièce d'identité fournie par le porteur via le service en ligne d'enregistrement. L'AE utilise un service externe (fourni par un prestataire de Cegedim) d'analyse de la pièce d'identité pour décider de valider ou non l'identité du porteur.

3.2.4 Informations non vérifiées du porteur

L'AE vérifie, pour certains parcours de signature, la validité de l'adresse de messagerie du porteur par l'envoi d'un lien unique à cette adresse, auquel le porteur doit répondre pour poursuivre le processus. Dans les autres cas, l'adresse de messagerie du porteur n'est pas vérifiée.

3.2.5 Validation de l'autorité du demandeur

Sans objet.

3.2.6 Certification croisée d'AC


Sans objet.

3.3 Identification et validation d'une demande de renouvellement

Dans le cadre de la présente politique, il n'y a pas de renouvellement de certificat.

3.4 Identification et validation d'une demande de révocation

Sans objet, le porteur ne peut pas réaliser de demande de révocation.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La demande de certificat est réalisée par une personne physique dans le cadre d'une cérémonie de signature d'un ou plusieurs documents.

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Le demandeur fournit, via l'entité créant la cérémonie de signature, les informations suivantes :

- Son nom et son prénom ;
- Son adresse courriel ;
- Son numéro de téléphone mobile.

La demande de certificat est établie par le futur porteur auprès du service en ligne de l'AE, au cours de la cérémonie de signature.

Niveau NCP

Le demandeur produit une pièce d'identité à l'opérateur de l'Autorité d'Enregistrement.

Niveau LCP

Le demandeur fournit une copie de sa pièce d'identité au service en ligne de l'AE.


4.2 Traitement d'une demande de certificat

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

L'Autorité d'Enregistrement effectue les opérations suivantes :

- Vérification de l'adresse courriel du demandeur par envoi d'un lien unique à cette adresse (optionnel) ;
- Authentification du demandeur par envoi d'un code à usage unique par messagerie ou sur le numéro de téléphone mobile ;
- Vérification de l'identité du demandeur selon le processus décrit au §3.2.3 ;
- Soumission pour acceptation des Conditions Générales d'Utilisation du certificat au demandeur ;
- Recueil du consentement du demandeur à signer le ou les documents ;
- Génération de la bi-clé du demandeur et de la requête de certificat ;
- Constitution et vérification de complétude du dossier d'enregistrement avec les éléments vérifiés ci-dessus ;
- Transmission de la demande de certificat à l'AC en cas de succès de toutes les phases précédentes ;
- Archivage du dossier de demande.

PUBLIC

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

4.2.2 Acceptation ou rejet de la demande

Le processus de demande est interrompu dès qu'une étape de vérification des informations du porteur échoue ou si le porteur refuse les Conditions Générales d'Utilisation du certificat.

L'AE peut notamment rejeter la demande :

- En cas d'incohérence entre l'identité attendue du demandeur et la pièce d'identité présentée ;
- Lorsque la pièce d'identité n'est plus valide ;
- S'il existe un doute sur l'authenticité de la pièce d'identité.

Dans tous ces cas d'erreur, l'AE ne transmet pas de demande de certificat à l'AC et en notifie le demandeur par courriel ou directement sur le service d'enregistrement en ligne.

4.2.3 Durée d'établissement du certificat

Le certificat est émis par l'AC immédiatement après réception et contrôle de la demande.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

L'Autorité de Certificat effectue les opérations suivantes :

- Authentification de l'origine de la demande ;
- Vérification d'intégrité de la demande ;
- Génération du certificat de signature pour le porteur ;
- Transmission du certificat au service en ligne de l'AE.

4.3.2 Notification de la délivrance du certificat au porteur

Le porteur est notifié de la délivrance du certificat de signature par l'information de succès de sa signature électronique.

4.4 Acceptation du certificat

L'acceptation du certificat par le porteur est tacite, à partir du moment où le demandeur a accepté les CGU du certificat et validé sa demande de certificat en demandant de signer.

4.4.1 Publication du certificat

Les certificats émis ne sont pas publiés.

4.4.2 Notification aux autres entités de la délivrance du certificat


L'AE reçoit le certificat dès que celui-ci a été généré.

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 de la clé privée du porteur et du certificat associé est strictement limitée à la signature à la volée de documents, pour la durée de la session de signature en cours.

Tout autre usage est interdit.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

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

Les utilisateurs du certificat peuvent vérifier la validité de la signature électronique des documents signés par le porteur, en exploitant les informations du certificat et de la liste de révocation mise à disposition par l'AC.

4.6 Renouvellement d'un certificat

Sans objet.

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

La délivrance d'un nouveau certificat au porteur nécessite de reproduire le même processus que la délivrance initiale.

4.8 Modification du certificat

La modification du certificat n'est pas permise.

4.9 Révocation et suspension des certificats

L'AC n'émet que des certificats de signature éphémères (durée de validité de 30 minutes). Conformément à la norme ETSI 319 411-1, l'AC a choisi de ne pas mettre en place de processus de révocation pour ces certificats étant donné la difficulté pratique de mise en place et la destruction de la clé privée dès la signature terminée.

L'AC publie toutefois une CRL qui peut être utilisée par les utilisateurs pour s'assurer de leur statut.

4.9.1 Causes possibles d'une révocation

Sans objet, les certificats des porteurs ne peuvent pas être révoqués.

4.9.2 Origine d'une demande de révocation

Sans objet, les certificats des porteurs ne peuvent pas être révoqués.

4.9.3 Procédure de traitement d'une demande de révocation

Sans objet, les certificats des porteurs ne peuvent pas être révoqués.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Sans objet, les certificats des porteurs ne peuvent pas être révoqués.

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

Sans objet, les certificats des porteurs ne peuvent pas être révoqués.


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, 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 publiés par Cegedim ;
- Le statut de révocation grâce aux CRL publiées par Cegedim (excepté pour les certificats éphémères qui ne peuvent pas être révoqués).

4.9.7 Fréquence d'établissement des CRL

Les CRL sont publiées quotidiennement.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

4.9.8 Délai maximum de publication d'une CRL

Le délai de 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).

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 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. De plus, en cas de compromission de sa clé privée, l'AC s'oblige à interrompre immédiatement et définitivement l'usage de sa clé privée et de son certificat associé. Conformément aux obligations réglementaires sur les prestataires de service de confiance européens, l'organe de contrôle national sera informé de la compromission d'une clé privée de l'AC dans les 24 (vingt-quatre) heures.

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 indiquée au §2.1.1.

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 PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

5 MESURES DE SECURITE NON TECHNIQUES

Se référer au document *Politiques et pratiques des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim*.

6 MESURES DE SECURITE TECHNIQUES

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

6.1 Gestion des clés des porteurs

6.1.1 Génération des bi-clés du porteur

Les clés des porteurs sont générées par le moteur de signature dans un environnement sécurisé.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet, la clé privée du porteur n'est pas transmise à son propriétaire.

6.1.3 Transmission de la clé publique à l'AC

La transmission de la clé publique du porteur vers l'AC est protégée en intégrité et en authenticité.

6.1.4 Taille des clés

Les bi-clés des porteurs sont des clés RSA de taille minimale de 2048 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 signature.

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

Sans objet.

6.2.2 Séquestre de la clé privée

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

6.2.3 Copie de secours de la clé privée

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

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

La clé privée du porteur est activée au moment de sa génération.

6.2.6 Méthode de désactivation de la clé privée

La clé privée d'un porteur est désactivée au moment de sa destruction.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

6.2.7 Méthode de destruction des clés privées

Les clés privées des porteurs sont détruites de façon sécurisée dès la fin de la session de signature.

6.3 Autres aspects de la gestion des bi-clés

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 bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente ont comme même durée de vie la durée de validité spécifiée dans le gabarit du certificat au §7.1.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les clés sont actives dès leur génération, déclenchée après l'authentification du porteur conformément aux mesures présentées aux §4.1 et §4.2.

6.4.2 Protection des données d'activation

Non applicable.

7 PROFILS DES CERTIFICATS ET DES CRL

7.1 Profil des certificats des porteurs pour le niveau NCP

Les certificats de signature de niveau NCP 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		E = <Adresse de messagerie du porteur> CN= <Prénom> <Nom> SERIALNUMBER = <Numéro unique de porteur> GN = <Prénom du porteur> SN = <Nom patronymique du porteur> C = FR
Emetteur		CN = CEGEDIM USER ADANCED CA OI = NTRFR-350422622 O = CEGEDIM C = FR
Durée de validité		30 minutes
Algorithme de clé publique		RSA
Longueur des clefs		2048 bits
Algorithme de signature		SHA512WithRSA
Extensions	Criticité	Valeur de l'extension
Basic Constraints	N	CA : Faux
Key Usage	O	Non Repudiation
Certificate Policies	N	1. PolicyIdentifier : 1.3.6.1.4.1.142057.10.4.1.1.1 Qualifier : CPS = http://psco.cegedim.com 2. PolicyIdentifier : 0.4.0.2042.1.1
SubjectAlternativeName	N	rfc822Name : <Adresse de messagerie du porteur>
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/CEGEDIMUSERADVANCEDCA.crt
CRL Distribution Points	N	URI de la CRL de l'AC : http://psco.cegedim.com/CRL/CEGEDIMUSERADVANCEDCA.crl

7.2 Profil des certificats des porteurs pour le niveau LCP

Les certificats de signature de niveau LCP 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		E = <Adresse de messagerie du porteur> CN= <Prénom> <Nom> SERIALNUMBER = <Numéro unique de porteur> GN = <Prénom du porteur> SN = <Nom patronymique du porteur> C = FR
Emetteur		CN = CEGEDIM USER ADANCED CA

PUBLIC

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		


	OI = NTRFR-350422622 O = CEGEDIM C = FR	
Durée de validité	30 minutes	
Algorithme de clé publique	RSA	
Longueur des clefs	2048 bits	
Algorithme de signature	SHA512WithRSA	
Extensions	Criticité	Valeur de l'extension
Basic Constraints	N	CA : Faux
Key Usage	O	Non Repudiation
Certificate Policies	N	1. PolicyIdentifier : 1.3.6.1.4.1.142057.10.4.2.1.1 Qualifier : CPS = http://psco.cegedim.com 2. PolicyIdentifier : 0.4.0.2042.1.3
SubjectAlternativeName	N	rfc822Name : <Adresse de messagerie du porteur>
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/CEGEDIMUSERADVANCEDCA.crt
CRL Distribution Points	N	URI de téléchargement de la CRL de l'AC : http://psco.cegedim.com/CRL/CEGEDIMUSERADVANCEDCA.crl

7.3 Profil du certificat de CEGEDIM USER ADVANCED CA

Le certificat de l'Autorité de Certification CEGEDIM USER ADVANCED 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 USER ADANCED CA OI = NTRFR-350422622 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

PUBLIC


	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

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

7.4 Profil des CRL de CEGEDIM USER ADVANCED CA


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

Champs de base		Valeur du champ
Version		1 (version 2)
Emetteur		CN = CEGEDIM USER ADANCED 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
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)

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Se référer au document *Politiques et pratiques des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim*.

	POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES LCP ET NCP	
V 1.4		

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

Se référer au document *Politiques et pratiques des services de confiance – Mesures de sécurité communes aux services eIDAS de Cegedim*.