POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES - STANDARD

Signé par:M. Jean-Marie SIMON
Date:11.10.2021 13:58:04 GMT
Package:FBF162C2033F

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	30/09/2021	30/09/2021	30/09/2021

HISTORIQUE DES VERSIONS

VERSION	DATE	AUTEUR	DESCRIPTIF DES MODIFICATIONS
1.2	27/09/2021	STEPHANE GALMICHE	PRECISIONS SUR LA CONSTITUTION DU DN
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

Table des matières

1 INTRODUCTION

Le présent document, *Politiques et pratiques de certification – AC Cegedim Personnes Physiques - Standard* présente les exigences spécifiques aux politiques de certification de l'AC ***CEGEDIM USER STANDARD 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.

Afin de faciliter la couverture des exigences normatives par les mesures décrites, chaque mesure est précédée des références aux exigences concernées.

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 de signature pour des personnes physiques, non certifiés selon la norme ETSI 319 411-1 du fait de l'absence de vérification de titre d'identité officiel par l'AC.

Ces certificats permettent de réaliser une signature électronique simple à la volée au sens du *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 ».

1.1 Identification de la PC

Le présent document intégre la politique de certification identifiée comme suit :

AC Emettrice	Type de certificat	Niveau eIDAS	OID de la PC
CEGEDIM USER STANDARD CA	Certificat de signature simple pour une personne physique	*aucun*	1.3.6.1.4.1.142057.10.6.1.1.1

La chaîne de certification est la suivante :

- CEGEDIM ROOT CA
  - CEGEDIM USER STANDARD CA
    - Certificats finaux de signature

1.2 Usage des certificats

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

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

1.3 Présentation du service et entités intervenant dans l'IGC

1.3.1 Autorité de Certification (AC)

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

Cegedim est la société portant l'autorité de certification ***CEGEDIM USER STANDARD 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 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 **Erreur ! Source du renvoi introuvable.**, 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

1.3.2 Autorité d'Enregistrement (AE)

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

- La vérification de l'intégrité des demandes de 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 ;
- La vérification des demandes de révocation de certificat.

La vérification des informations d'identité du porteur est à la charge de l'entité cliente de Cegedim. L'AE, selon le processus choisi par le client, peut toutefois vérifier l'adresse de messagerie électronique et/ou le numéro de téléphone portable du porteur dans le cadre de la cérémonie de signature.

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

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

- L'AE vérifie l'identité du Porteur par un code à usage unique envoyé sur le mobile de celui-ci;
- L'AE demande la révocation du Certificat Porteur dès qu'un événement anormal, précisé au **Erreur ! Source du renvoi introuvable.**, 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.

1.3.3 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 le demande de Certificat ;
- Accepter que le moteur de signature Cegedim génère, utilise puis détruise 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 téléphone mobile sur lequel il reçoit le code d'authentification à usage unique ;
- Demander sans délai la révocation de son Certificat s'il constate une erreur ou une fraude concernant son Certificat ;
- Accepter la conservation par l'AE et l'AC du dossier d'enregistrement et des journaux d'événements relatifs à son Certificat, afin de les produire comme preuve, le cas échéant en justice ;

Respecter, plus largement, les obligations qui lui incombent dans le cadre des présentes CGU et de la Politique de Certification associée.

1.3.4 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.

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/CEGEDIMUSERSTANDARDCA.crl

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	
SURNAME	
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 « TEST » placé en début du champ CN (c'est-à-dire devant le prénom du porteur).

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 pour la 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 du client.

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 ne vérifie pas l'identité du porteur, mais seulement et optionnellement l'adresse de messagerie (via un lien unique envoyé sur cet adresse) et le numéro de téléphone portable (via un OTP SMS) du porteur.

3.2.4 Informations non vérifiées du porteur

Les informations du porteur sont :

- Nom et prénom
- Adresse de messagerie
- Numéro de téléphone portable

Le nom et le prénom sont fournis par le créateur de la cérémonie de signature, les autres informations ne sont pas systématiquement vérifiées par l'AE mais doivent l'être par le client qui déclenche la cérémonie de signature.

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

Le porteur peut demander la révocation de son certificat en contactant l'AC par courriel.

L'AE authentifie le porteur par l'adresse de messagerie de l'expéditeur.

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 (optionnel).

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.

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 sur le numéro de téléphone mobile (optionnel) ;
- Soumission 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 vérifiation 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.

4.2.2 Acceptation ou rejet de la demande

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

En 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

La certificat est émis par l'AC immédiatement après réception 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.

Lorsque le certificat a été émis, le porteur peut en demander sa révocation (pour différentes raisons) selon les modalités décrites au §4.9.

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 biclé 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.

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

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 délivré ;
- La clé privée du porteur est suspectée de compromission, est compromise ou est perdue ;
- Les données d'authentification du porteur ont été compromises ;
- Le porteur demande la révocation de son propre certificat ;
- L'AC émettrice du certificat doit être révoquée ;
- Une rupture technologique nécessite de procéder à la génération de nouvelles biclés (longueurs ou algorithme 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), le certificat concerné doit être révoqué.

4.9.2 Origine d'une demande de révocation

Les personnes pouvant demander une révocation de certificat sont :

- Le porteur ;
- L'AE ;
- L'AC.

4.9.3 Procédure de traitement d'une demande de révocation

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

- Le nom et le prénom du porteur tels qu'ils apparaissent dans le certificat ;
- L'adresse courriel du porteur telle qu'indiquée à son enregistrement.

Les exigences d'identification et de validation effectuée par la fonction de gestion des révocations sont décrites au 3.4. Lorsque la demande est faite par l'AE ou l'AED, la demande doit être émise directement à l'AC qui en authentifie l'origine

L'AC contrôle que le certificat est bien identifié par la demande et qu'il est encore valide.

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.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur 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, 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.

4.9.7 Fréquence d'établissement des CRL

Les CRL sont publiées quotidiennement.

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 de porteur, le porteur et 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.

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 règlementaires 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.

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.

5 MESURES DE SECURITE NON TECHNIQUES

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

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 USER STANDARD 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 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 déactivée au moment de sa destruction.

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 la 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

Les certificats de signature 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>* GN = *<Prénom du porteur>* SN = *<Nom patronymique du porteur>* SERIALNUMBER = *<Numéro unique de porteur>* C = FR	
Emetteur	CN = CEGEDIM USER STANDARD CA OI = NTRFR-350422622 O = CEGEDIM C = FR	
Durée de validité	30 minutes	
Algorithe 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	PolicyIdentifier : 1.3.6.1.4.1.142057.10.6.1.1.1 Qualifier : CPS = http://psco.cegedim.com/CPS
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-caIssuers accessLocation : http://psco.cegedim.com/CRT/CEGEDIMUSERSTANDARDCA.crt
CRL Distribution Points	N	URI de la CRL de l'AC : http://psco.cegedim.com/CRL/CEGEDIMUSERSTANDARDCA.crl

Les attributs SN et GN sont facultatifs dans le sujet. Dans ce cas le CN est une valeur fournie par l'entité créant la cérémonie de signature et est sous la responsabilité de l'entité.

7.2 Profil du certificat de CEGEDIM USER STANDARD CA

Le certificat de l'Autorité de Certification CEGEDIM USER STANDARD 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 STANDARD 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	
Algorithe 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-caIssuers 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 de CEGEDIM USER STANDARD CA

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

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

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

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