POLITIQUES ET PRATIQUES DE CERTIFICATION AC CEGEDIM PERSONNES PHYSIQUES - QCP-N-QSCD

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
1.3	01/06/2023	STEPHANE GALMICHE	CORRECTION D'UNE INCOHERENCE SUR LA TAILLE DE CLE MINIMALE DES PORTEURS
1.2	17/05/2023	STEPHANE GALMICHE	VERIFICATION D'IDENTITE A DISTANCE PAR UN MIE OU UN SERVICE PVID CERTIFIE SUPPRESSION DE L'AED
1.1	05/05/2021	STEPHANE GALMICHE	AJOUT DE L'EXTENSION SUBJECTALTERNATIVENAME CORRECTIONS MINEURES
1.0	15/04/2021	STEPHANE GALMICHE	VERSION INITIALE

Signé par:Hong GIRAULT
Date:13.09.2023 13:15:09 GMT
Package:6D7132808A09

Table des matières

1 INTRODUCTION

1.1 Présentation générale

Le présent document, *Politiques et pratiques de certification – AC Cegedim Personnes Physiques - QCP-n-qscd* présente les exigences spécifiques aux politiques de certification de l'AC ***CEGEDIM USER 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 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 qualifiés de signature sur support qualifié pour des personnes physiques en lien avec une personne morale, de niveau QCP-n-qscd (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 une signature électronique qualifiée au sens du Règlement eIDAS, ainsi que de s'authentifier sur un site distant en TLS.

1.2 Identification de la PC

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

AC Emettrice	Type de certificat	Niveau eIDAS du certificat	OID de la PC
CEGEDIM USER QUALIFIED CA	Certificat qualifié de signature sur support qualifié et d'authentification pour une personne physique	Niveau QCP-n-qscd 0.4.0.194112.1.2	1.3.6.1.4.1.142057.10.2.1.1.1

La chaîne de certification est la suivante :

- CEGEDIM ROOT CA
  - CEGEDIM USER QUALIFIED CA
    - Certificats finaux de niveau QCP-n-qscd

1.3 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.

1.4 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 la fait appliquer, garantissant ainsi un niveau de confiance défini aux utilisateurs.

Cegedim est la société portant l'autorité de certification ***CEGEDIM USER 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 génération des éléments secrets du porteur (sur le QSCD) ;
- 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 des demandeurs de certificat, afin de garantir la validité des informations contenues dans le certificat ;
- La constitution du dossier d'enregistrement suite aux vérifications ci-dessus ;
- La remise du support QSCD au porteur ;
- L'archivage des dossiers d'enregistrement de certificat ;
- La vérification des demandes de révocation de certificat.

La vérification de l'identité du porteur est réalisée par l'une des méthodes suivantes :

- Vérification d'identité en face à face : un face à face physique est organisé par un opérateur d'une Autorité d'Enregistrement Déléguée ou de l'Autorité d'Enregistrement ;
- Vérification d'identité à distance par un service PVID : l'AE délègue la vérification d'identité à distance à un prestataire certifié PVID au niveau substantiel ;
- Vérification d'identité à distance par un MIE : l'AE réalise la vérification d'identité à distance en recourant à une identification électronique par un Moyen d'identification électronique (MIE) de niveau de garantie substantiel.

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

Le porteur de certificat est une personne physique qui demande un certificat de signature pour elle-même, en relation avec une entité (personne morale) avec laquelle elle a un lien contractuel, hiérarchique ou réglementaire.

La fiabilité de la signature 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 ses données d'identité dans la demande de Certificat ;
- Générer sa biclé (clé RSA de taille minimale de 4096 bits) dans un dispositif cryptographique qualifié et selon les modalités définies dans la Politique de Certification ;
- Assurer la sécurité et le contrôle exclusif de son dispositif cryptographique ;
- Garantir la confidentialité de son code PIN et des réponses aux questions de sécurité qu'il a choisies ;
- 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.

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 ou authentifier le porteur qui présente ce certificat lors d'une authentification TLS.

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 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/CEGEDIMUSERQUALIFIEDCA.crl

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Identification des porteurs

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*
SERIAL NUMBER	*Numéro unique affecté à la demande de certificat*
GIVEN NAME	*Prénom du porteur*
SURNAME	*Nom du porteur*
ORGANIZATION IDENTIFIER	*Identifiant unique de l'entité conforme à la norme ETSI EN 319 412-1* *En France, ce numéro est de la forme : NTRFR-<SIREN ou SIRET>*
ORGANIZATION	*Dénomination sociale de l'entité à laquelle est rattaché le porteur, telle qu'elle est indiquée sur les justificatifs d'identité présentés à l'enregistrement*
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.

3.1.2 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.

3.1.3 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

Sans objet. Le porteur ne génère pas sa clé privée.

3.2.2 Validation de l'identité d'un organisme

L'AE valide le lien du porteur avec l'entité à laquelle il sera attaché dans le certificat par une pièce justificative, valide au moment de l'enregistrement, attestant de l'existence de l'entité et par un document ou une preuve du lien entre le porteur et cette entité.

La pièce justificative d'existence de l'entreprise peut porter le numéro SIREN de celle-ci (un extrait Kbis par exemple), ou, à défaut, attester l'identification unique de celle-ci. Pour une administration, cette pièce doit porter délégation ou subdélégation de l'autorité responsable de la structure administrative.

La preuve du lien peut être constituée par un document attestant de la qualité du demandeur de certificat et signé par une personne autorisée de cette entité.

3.2.3 Validation de l'identité d'un individu

Vérification d'identité en face à face : 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.

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.

Vérification d'identité à distance par un service PVID : Le portail d'enregistrement de l'AE dirige le porteur vers un service de vérification d'identité à distance.

Vérification d'identité à distance par un MIE : Le portail d'enregistrement de l'AE demande au porteur de s'identifier en utilisant un Moyen d'identification électronique

3.2.4 Informations non vérifiées du porteur

Sans objet.

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

Le renouvellement d'un certificat peut être demandé par le porteur 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

Le porteur peut demander la révocation de son certificat sur le portail en ligne de l'AE ou bien transmettre à l'AE un formulaire renseigné de demande de révocation.

Sur le portail en ligne de l'AE, le porteur s'authentifie en répondant à des questions de sécurité dont il a indiqué les réponses secrètes au moment de son enregistrement.

Un formulaire renseigné de demande de révocation doit 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 :

- Numéro de série du certificat ;
- 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…)

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

La demande de certificat est réalisée par une personne physique auprès d'une Autorité d'Enregistrement.

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 porteur initie sa demande de certificat :
    a. Vérification d'identité en face à face
        i. Le porteur se présente en face à face à l'AE avec une pièce d'identité et les preuves de son lien avec l'entité avec laquelle il sera rattaché dans le certificat ;
        ii. L'opérateur AE vérifie l'identité du porteur ;
    b. Vérification d'identité à distance par un service PVID
        i. Le porteur se connecte sur le portail de l'AE, saisit ou télécharge les informations demandées ;
        ii. Le porteur est redirigé par le portail sur un service PVID de niveau de garantie substantiel et suit le parcours de vérification d'identité à distance ;
    c. Vérification d'identité à distance par un MIE
        i. Le porteur se connecte sur le portail de l'AE, saisit ou télécharge les informations demandées ;
        ii. Le porteur s'authentifie avec un Moyen d'identification électronique de niveau de garantie substantiel et autorise l'envoie de ses informations d'identité au portail de l'AE ;
2. L'opérateur AE vérifie l'identité de l'entité de rattachement et son lien avec le porteur ;
3. LAE établit le formulaire de demande en reportant au minimum :
    a. Le nom et prénom du porteur ;
    b. L'adresse de courriel du porteur ;
    c. Le numéro de téléphone mobile du porteur ;
    d. Le type de pièce d'identité présentée, son numéro, sa date de validité et l'autorité de délivrance ;
    e. L'identification de l'entité de rattachement et, optionnellement, l'identifiant du porteur dans cette entité.
4. L'AE présente, en face à face ou à distance par le portail AE, le formulaire de demande au porteur et lui demande de vérifier l'exactitude de ces informations ;
5. L'AE présente les CGU au porteur et lui demande de les accepter ;
6. Le porteur signe électroniquement le formulaire de demande et les CGU ;
7. L'AE archive le dossier d'enregistrement comprenant :
    a. Le formulaire de demande signé par le porteur ;

b. Les CGU signées par le porteur ;

c. Les preuves du lien du porteur avec l'entité de rattachement.

8. Vérification d'identité à distance par un service PVID et Vérification d'identité à distance par un MIE : L'opérateur AE prend rendez-vous avec le porteur pour effectuer une remise du dispositif cryptographique en main propre. Lors de ce rendez-vous en face à face, l'opérateur AE commence par vérifier l'identité du porteur qui se présente par rapport au dossier constitué ;

9. Le porteur se connecte sur le portail de l'AE, depuis un poste mis à disposition par l'opérateur AE en face à face physique avec lui :

   a. Le porteur connecte le dispositif cryptographique remis par l'AE ;

   b. Le porteur entre le code d'activation qu'il a reçu de l'AE par courriel ;

   c. Le porteur saisit les réponses à au moins trois questions de sécurité, à utiliser pour une demande de révocation en ligne ;

   d. Le porteur choisit son code PIN ;

   e. La biclé du porteur est générée sur son dispositif cryptographique (QSCD) ;

   f. Le certificat généré par l'AC est inscrit sur le dispositif cryptographique du porteur.

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 que le porteur refuse les Conditions Générales d'Utilisation du certificat.

L'AE peut notamment rejeter la demande :

- En cas d'incohérence entre l'identité du demandeur et les pièces présentées ;
- Lorsque la pièce d'identité n'est plus valide ;
- S'il existe un doute sur l'authenticité des pièces ;
- Si les preuves du lien avec l'entité de rattachement sont insuffisantes ou erronées.

Dans tous ces cas d'erreur, l'AE ne transmet pas de demande de certificat à l'AC et en notifie le demandeur.

4.2.3 Durée d'établissement du certificat

La certificat est émis par l'AC lors du face à face avec l'AE.

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 (CSR transmise par l'AE) ;
- Vérification d'intégrité de la demande ;
- Génération du certificat de signature pour le porteur ;
- Renvoi du certificat à l'AE.

4.3.2 Notification de la délivrance du certificat au porteur

Le porteur est informé par l'opérateur AE de la fin de génération du certificat de signature sur son dispositif cryptographique.

4.4 Acceptation du certificat

Le porteur et l'opérateur de l'AE vérifient les informations du certificat délivré par l'AC. 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.

Plus tard, le porteur peut demander la révocation du certificat (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 est informé de la génération du certificat dès que celui-ci a été inscrit sur le dispositif.

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 électronique ou à l'authentification client TLS.

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

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

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

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

Le renouvellement est réalisé en suivant la procédure de demande 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 ;
- Le lien entre le porteur et l'entité de rattachement est rompu ;
- Les données d'authentification du porteur ont été compromises ;
- Le porteur demande la révocation de son propre certificat ;
- Révocation de l'AC ;
- Rupture technologique, nécessitant de procéder à la génération de nouvelles biclés (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 une révocation de certificat sont :

- Le porteur ;
- Un responsable légal de l'entité de rattachement ;
- L'AE ;
- L'AC.

4.9.3 Procédure de traitement d'une demande de révocation

La demande de révocation doit identifier le certificat à révoquer par son numéro de série, ou bien par les nom, prénom et dates de validité apparaissant dans le certificat.

Les exigences d'identification et de validation effectuée par la fonction de gestion des révocations sont décrites au 3.4. Après authentification, le porteur sélectionne le certificat à révoquer et le portail de l'AE transmet la demande de révocation à l'AC.

Lorsque le porteur n'a plus les réponses aux questions de sécurité, le porteur doit s'authentifier auprès de l'AE qui relaie la requête à l'AC après authentification du porteur. Lorsque la demande est faite par l'AE, elle doit être émise directement à l'AC.

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, l'état 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 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 QUALIFIED CA ».

6.1 Gestion des clés des porteurs

6.1.1 Génération des bi-clés du porteur

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

6.1.2 Transmission de la clé privée à son propriétaire

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

6.1.3 Transmission de la clé publique à l'AC

La transmission de la clé publique du porteur depuis l'AE 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 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 signature et d'authentification client TLS.

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 pour les clés privées des porteurs.

Se référer au document *Politiques et pratiques des services* ***de*** *confiance – Mesures de sécurité communes aux services eIDAS de Cegedim* pour les clés privées de l'AC.

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

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

6.2.6 Méthode de désactivation de la clé privée

Les conditions de désactivation de la clé privée d'un porteur permettent de répondre aux exigences définies au §10.1.

6.2.7 Méthode de destruction des clés privées

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.

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

Le porteur génère lui-même ses données d'activation.

6.4.2 Protection des données d'activation

Le porteur est responsable de la protection de ses données d'activation.

7 PROFILS DES CERTIFICATS ET DES CRL

7.1 Profil des certificats des porteurs pour le niveau QCP-n-qscd

Les certificats de signature de niveau QCP-n-qscd 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 demande de certificat*> GN = <*Prénom du porteur*> SN = <*Nom patronymique du porteur*> OI = <*Identifiant de l'entité de rattachement, conforme à la norme ETSI EN 319 412, en France de la forme NTRFR-<SIREN ou SIRET>* > O = <*Entité de rattachement du porteur*> C = FR	
Emetteur	CN = CEGEDIM USER 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**	**Valeur de l'extension**
Basic Constraints	N	CA : Faux
Key Usage	O	Non Repudiation et DigitalSignature
Extended Key Usage	N	clientAuth et emailProtection
Certificate Policies	N	1. PolicyIdentifier : 1.3.6.1.4.1.142057.10.2.1.1.1 Qualifier : CPS = http://psco.cegedim.com 2. PolicyIdentifier : 0.4.0.194112.1.2
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/CEGEDIMUSERQUALIFIEDCA.crt
CRL Distribution Points	N	URI de la CRL de l'AC : http://psco.cegedim.com/CRL/CEGEDIMUSERQUALIFIEDCA.crl
qcStatements	N	esi4- qcStatement-1 = id-etsi-qcsQcCompliance esi4- qcStatement-4 = id-etsi-qcs-QcSSCD esi4- qcStatement-6 = id-etsi-qct-esign

7.2 Profil du certificat de CEGEDIM USER QUALIFIED CA

Le certificat de l'Autorité de Certification CEGEDIM USER 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 USER QUALIFIED 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
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 QUALIFIED CA

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

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

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*.

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*.

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.

Le dispositif cryptographique du porteur doit avoi été notifié comme QSCD (Qualified Signature Creation Device) au sens du règlement eIDAS.