MINISTÈRE
DE L'ÉDUCATION
NATIONALE
ET DE LA JEUNESSE
Liberté
Égalité
Fraternité

Plateforme Nationale de Confiance Numérique

Condition Générales d'Utilisation
Pour les certificats de signature de personnes physiques et de personnes morales

CGU AC Signature – Format RFC 3647

Statut du document : validé
Version : 2.1

PUBLIE

Entrée en vigueur le 09/07/2024

Table des matières

1 INTRODUCTION

Le présent document définit l'ensemble des Conditions d'Utilisation des Certificats émis par l'AC SIGNATURE du Ministère de l'Education Nationale (MEN).

2 IDENTIFICATION DU DOCUMENT

Le numéro d'OID du présent document est 1.2.250.1.535.2.2.2.4.3.1.3
Les profils de certificats suivants sont émis à travers la Politique de Certification :

1.2.250.1.535.2.2.2.4.6.1.1	Infrastructures_Cachet_Serveur
1.2.250.1.535.2.2.2.4.6.2.1	Personnes_Signature
1.2.250.1.535.2.2.2.4.6.3.1	Personnes_Signature_Materiel
1.2.250.1.535.2.2.2.4.6.4.1	OCSP_Signatures
1.2.250.1.535.2.2.2.4.6.5.1	Personnes_Signature_Mail_Logiciel
1.2.250.1.535.2.2.2.4.6.8.1	Certificat_Ephémères_Signatures
1.2.250.1.535.2.2.2.4.6.9.1	Personnes_Signature_SCEP

3 GESTION D'AUTORITE DE CERTIFICATION

3.1 ENTITE GERANT L'AUTORITE DE CERTIFICATION

L'Autorité de Certification est de la responsabilité du sous-directeur du MEN— socle 4. Pour cela la gouvernance est assurée à travers le « Bureau de la sécurité » et son Comité de Suivi des Services de Confiance (C2SC).

3.2 POINT DE CONTACT

Toutes questions concernant les activités d'émission de certificats du MEN sont à adresser à l'adresse email suivante : service.certification@pncn.education.gouv.fr.

4 DEFINITIONS ET ACRONYMES

4.1 ACRONYMES

AC	**A**utorité de **C**ertification
AE	**A**utorité d'**E**nregistrement
C2SC	**C**omité de **S**uivi des **S**ervices de **C**onfiance
COSSIM	**C**omité **S**écurité des **S**ystèmes d'**I**nformation du **M**inistère
DN	**D**istinguished **N**ame
DNE	**D**irection du **N**umérique pour l'**E**ducation
DPC	**D**éclaration de **P**ratiques de **C**ertification
ETSI	Institut européen des normes de télécommunication (**E**uropean **T**elecommunications **S**tandards **I**nstitute)
IGC	**I**nfrastructure de **G**estion de **C**lés
LCR	**L**iste des **C**ertificats **R**évoqués
MEN	**M**inistère de l'**E**ducation **N**ationale de la **J**eunesse
PNCN	**P**lateforme **N**ationale de **C**onfiance **N**umérique
OID	Identifiant d'objet (**O**bject **ID**entifier)
OCN	**O**fficier de **C**onfiance **N**umérique
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol
OSC	**O**pérateur de **S**ervice de **C**ertification
PC	**P**olitique de **C**ertification
PSCo	**P**restataire de **S**ervice de **Co**nfiance
Qcp	Qualified Certificate Policy
QSCD	Dispositif de Création de Signature Qualifié (**Q**ualified **S**ignature **C**reation **D**evice)
RCC	**R**esponsable du **C**ertificat de **C**achet
SIEM	**S**ecurity **I**nformation **E**vent **M**anagement
SOCLE 4	Bureau de la sécurité numérique et du centre opérationnel de sécurité des systèmes d'information ministériels – de la sous-direction SOCLE de la DNE

4.2 DEFINITIONS

Authentification : Processus permettant de vérifier l'identité déclarée d'une personne ou de tout autre entité, ou de garantir l'origine de données reçues.

Autorité de certification : Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer des certificats.

Bi clé : Un bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.

Certificat : Clé publique d'un utilisateur, concaténée à d'autres informations rendues infalsifiables par signature avec la clé privée de l'autorité de certification qui l'a délivré.

Certificat d'AC : Certificat d'une autorité de certification.

Certificat de cachet : Certificat final disposant des usages permettant de faire du cachet électronique. Le certificat est émis au nom d'une personne morale

Certificat de signature : Certificat final disposant des usages permettant de faire de la signature électronique. Le certificat est émis au nom d'une personne physique

Déclaration des pratiques de certification : Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats

Données d'activation : Données privées associées à un RCC permettant d'initialiser ses éléments secrets.

Infrastructure de Gestion de Clés : Ensemble de composantes fournissant des services de gestion de clés et de certificats au profit d'une communauté d'utilisateurs.

Liste d'Autorités Révoqués : Liste contenant les identifiants des certificats d'Autorités de Certification révoqués ou invalides.

Liste de Certificats Révoqués : Liste contenant les identifiants des certificats révoqués ou invalides.

OCN : Officier de **C**onfiance **N**umérique. Rôle de confiance travaillant au sein d'une AE pour gérer les cycles de vie des certificats

Partenaires : Toutes entités ou personnes qui utilisent les certificats émis par le MEN.

Politique de certification : Ensemble de règles relatives à l'applicabilité d'un certificat à une communauté et / ou à une classe d'applications ayant des besoins de sécurité communs.

Serveur OCSP : Serveur connecté à la base de données des certificats et permettant de fournir en temps réel le statut d'un certificat électronique

5 REFERENCES DOCUMENTAIRES

[eIDAS] : Règlement européen n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

[CNIL] : Commission nationale de l'informatique et des libertés

[RGPD] : Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[PC] : Politique de Certification de l'AC SIGNATURE

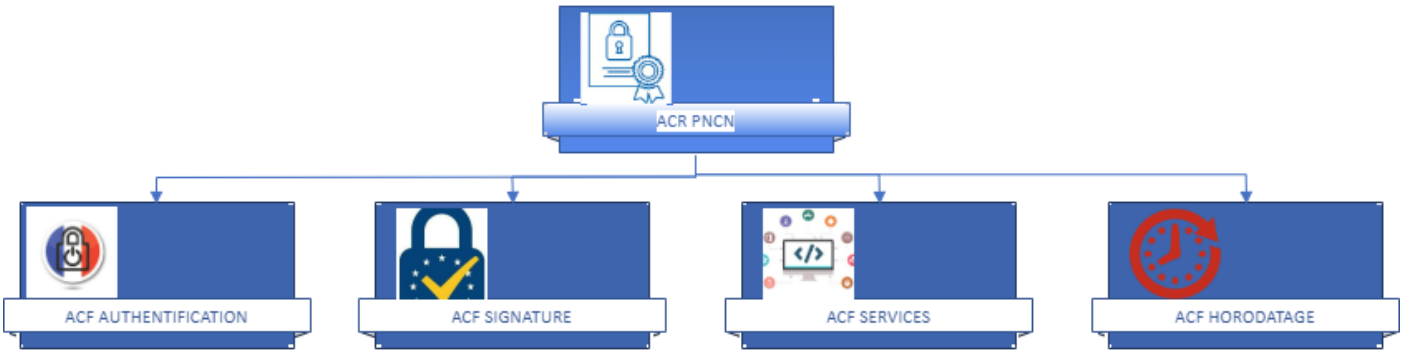
[DPC] : Déclaration des Pratiques commune à l'ensemble des AC du MEN.

6 ENTITES INTERVENANT DANS L'IGC

Le certificat de l'AC SIGNATURE est mis en œuvre pour :

- Signer les demandes de certificats des certificats finaux
- Signer la Liste des Certificats Révoqués (LCR)
- Signer les demandes de certificats OCSP.

La hiérarchie d'Autorités de Certification mise en œuvre est la suivante :



Le prestataire de service de certification électronique (PSCE) est le MEN. Il est dans ce cadre également l'autorité de certification (AC), autorité à laquelle les utilisateurs des services de certification accordent leur confiance pour la création et l'émission des certificats.

Le MEN a recouru au pôle PNCN en tant qu'Opérateur de Service de Certification (OSC), pour opérer les fonctions de gestion des certificats.

6.1 AUTORITES DE CERTIFICATION

Le MEN est l'autorité de certification. Il est sous la responsabilité du sous-directeur de la DNE – Socle Numérique.
Il est en charge de l'application de la politique de certification.
L'AC fournit des prestations de gestion des certificats aux agents du MEN ainsi qu'à certains partenaires.
Les bi clés et certificats considérés dans le présent document sont utilisés en support de la fonction de signature. Ce sont :

- Les bi-clés et certificats générés sur des supports cryptographiques matériels permettant la signature de document électronique dans différents formats,
- Les bi-clés et certificats générés sous format logiciel permettant la signature de données au format électroniques
- Les bi-clés et certificats de cachets opérés par la PNCN et stockés dans des environnements cryptographiques matériels.

Chaque certificat final possède un OID spécifique en complément de l'OID de la PC dans le champ « Politique de Certification » qui précise à quel sous-ensemble il appartient et comme cela est décrit dans le paragraphe 2.

6.2 OPERATEUR DE SERVICE DE CERTIFICATION

L'opérateur de service de certification est la PNCN. Il est en charge du maintien en conditions opérationnelles et en conditions de sécurité de l'ensemble des composants constituant la PNCN. Cela comprend notamment :

- Les fonctions de génération des certificats
- La fonction de remise au porteur de ses éléments de protection de la clé privée de son certificat
- La fonction de publication des informations
- La fonction de gestion des révocations
- La fonction d'information sur l'état des certificats

6.3 AUTORITE D'ENREGISTREMENT (AE)

Il s'agit de l'entité du service de confiance en charge de gérer le cycle de vie des certificats. L'Autorité d'Enregistrement opère son rôle en délégation de l'AC. Cette délégation, et les tâches associées, sont établies dans un contrat de mandat AC – AE.
L'Autorité d'Enregistrement est opérée par la PNCN au travers de ses Officiers de Confiance Numérique

6.4 OFFICIER DE CONFIANCE NUMERIQUE (OCN)

Il s'agit des opérateurs de saisie et de validation des demandes de certificats.
Il existe 2 types d'OCN :

- OCN central
- Un OCN central ne peut être qu'un membre de la PNCN ou de SOCLE 4
- OCN de proximité
- Un OCN de proximité est une personne située dans les services académiques et à l'administration centrale.

Suivant les gammes de certificats concernées, seul un OCN central pourra assurer leur validation.

6.5 PORTEURS DE CERTIFICATS

Les porteurs de certificats sont des agents du Ministère ou des personnes contractuellement liées au Ministère.

6.6 RESPONSABLE DE CERTIFICATS DE CACHETS (RCC)

Il s'agit de personnes au sein de la PNCN en charge d'assurer la gestion des certificats de cachets qui sont mis en œuvre sur des serveurs de la PNCN. Ce rôle est explicitement mentionné dans la demande de certificat.

6.7 UTILISATEURS DE CERTIFICATS

Les certificats couverts par les présentes CGU sont utilisés dans les applications métiers mis en œuvre par le MEN ou ses partenaires. Il s'agit donc d'application métiers ayant des besoins de signatures ou de cachets électroniques.

7 NIVEAU ET USAGE DES CERTIFICATS

7.1 NIVEAU DES CERTIFICATS EMIS

Les certificats couverts par les présentes CGU ont les niveaux suivants :

- Qcp-n
- Qcp-l
- Qcp-n-qscd

7.2 DOMAINES D'UTILISATION APPLICABLES

Les certificats finaux sont utilisés soit pour produire des signatures électroniques soit pour produire des cachets électroniques dans le cadre de ses activités professionnelles et dans le respect des délégations de signature établies.

7.3 DOMAINES D'UTILISATION INTERDITS

En dehors des usages identifiés dans le paragraphe précédent, tous les autres usages ne sont pas couverts par les présentes CGU.

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

8.1 ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS

L'AC est chargée de la mise à disposition de la politique de certification, de la déclaration des pratiques de certification et des conditions générales d'utilisation.
Ces informations sont accessibles via Internet, sur le site géré par la PNCN : http://igc.pncn.education.gouv.fr/
L'accès à ce service est assuré 24h/24 et 7j/7 avec un taux de disponibilité de 99%.

8.2 INFORMATIONS DEVANT ETRE PUBLIEES

Les informations publiées sont les suivantes :

- La Politique de Certification ainsi que la Politique de Certification de l'AC Racine « AC PNCN »
- Les Conditions Générales d'Utilisation des certificats finaux
- La liste des Autorités Révoquées (LAR) pour les certificats d'AC
- La liste des certificats révoqués (LCR) pour les certificats des porteurs
- Les certificats de l'AC SIGNATURE en cours de validité, ainsi que les certificats en cours de validité de l'AC PNCN (hiérarchie à laquelle est rattachée l'AC SIGNATURE)
- Le condensat SHA256 du certificat auto signé de l'AC PNCN, permettant aux utilisateurs de s'assurer de l'origine et de l'état des certificats de l'AC PNCN

Les formulaires d'enregistrement, de renouvellement et de révocation sont directement téléchargeables sur le site de publication par les porteurs.
Les documents PC et CGU sont publiés :

- Au format PDF/A
- En français.

8.3 DELAIS ET FREQUENCES DE PUBLICATION

Les CGU sont revues si besoin et publiées au moins tous les deux ans.
Les certificats d'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats ou de LCR, dans un délai de 72 heures.
La fréquence de publication des LCR est compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication. Les LCR sont publiées toutes les 24h au moins.

8.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'accès en lecture est disponible pour tous.

9 MODALITES D'OBTENTION D'UN CERTIFICAT

9.1 NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms pour distinguer les titulaires sont explicites. Le nom distinctif est sous la forme d'une chaîne de type UTF8string de type nom X 501, excepté le champ serialNumber qui est en printableString.
Les informations portées dans le champ « Subject DN » du certificat sont décrites ci-dessous de manière explicite :

- Communs à tous les types de certificats :
  - Le Pays est positionné dans le champ « Country »
  - L'organisation d'appartenance est positionnée dans le champ « organization »
  - L'identifiant de l'organisation d'appartenance est positionné dans un champ « organizationalUnit » et dans le champ « organizationIdentifier »
  - L'unité d'appartenance est positionnée dans un ou plusieurs champ(s) « organizationalUnit »
- Spécifiques aux certificats de personnes :
  - Des éléments de localisation de la région académique dans le champ « state » et de l'académie dans le champ « locality »
  - Le nom de famille est positionné dans le champ « surName »
  - Le prénom est positionné dans le champ « givenName »
  - Le prénom et le nom sont concaténés dans le champ « commonName »
  - L'unicité du certificat est portée dans le champ « serialNumber » qui contient les informations de l'adresse email du porteur en remplaçant le caractère '@' par la suite de caractère 'at'
- Spécifiques aux certificats de cachets
  - L'unité ou le FQDN dans le champ « commonName »

Les champs en *italique* sont positionnés que pour certains profils.

9.2 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOMS

Les informations portées dans les certificats sont issues des justificatifs fournis dans le dossier de demande de certificats.
Notamment :

- Les noms et prénoms des personnes sont identiques à ceux présents complètement et strictement dans le justificatif d'identité
- Le nom de l'organisation, l'identifiant d'organisation sont ceux présents strictement dans le justificatif d'organisation

Concernant les certificats de cachet l'AE centrale s'assure que le nom porté dans la demande de certificat est bien fourni par un RCC habilité, et ne présente pas d'ambigüité sur l'interprétation du nom demandé dans le champ « commonName ».

9.3 UNICITE DES NOMS

Le champ « serialNumber » des certificats permet de garantir l'unicité des certificats à travers l'unicité du « DN ». L'information portée dans ce champ est basée sur l'adresse email du porteur de certificat avec un remplacement du caractère '@' par la chaîne de caractère 'at'.

L'IGC assure l'unicité des certificats cachet sur la base du contenu du DN avec un paramétrage technique sur la PKI qui n'autorise qu'un seul certificat à l'instant T avec ce DN.
Un même DN peut être présent dans plusieurs certificats en même temps, chacun des certificats correspondants étant délivrés au même porteur.

9.4 VALIDATION INITIALE DE L'IDENTITE

9.4.1 Méthode pour prouver la possession de la clé privée

9.4.1.1 Pour les certificats de personnes sur support matériel

Le futur porteur de certificat se voit remettre un support cryptographique au moment du face-à-face avec l'OCN. La clé privée est générée directement dans le support cryptographique au moment du traitement de la demande par l'OCN, en présence du futur porteur.
Ce dernier initialise un code PIN pour le support qui lui est remis au moment de la procédure de retrait du certificat. Ce code PIN lui est personnel et reste sous son contrôle exclusif.
Le niveau de qualification de la technologie utilisée permet de s'assurer de la possession de la clé privée par le support cryptographique du porteur, qui est protégée dès sa génération.

9.4.1.2 Pour les certificats logiciels

L'identité du futur porteur est fourni à travers la demande du porteur. Il n'est pas exigé pour ce type de certificats de justificatifs d'identité. L'OCN reçoit ses éléments par email soit de manière unitaire (1 seul certificat à produire) soit en masse (liste de certificats à produire).

9.4.1.3 Pour les certificats de cachet

Le RCC génère préalablement la clé privée sur l'équipement sur lequel le certificat de cachet sera installé. Cette génération est faite sous la responsabilité du RCC. Lors de la phase de vérification du dossier de demande avec l'OCN central, le RCC fournit une demande de certificat technique signée par la clé privée générée sur l'équipement sur lequel le certificat cachet sera installé.

9.4.2 Validation de l'identité d'un organisme

Les certificats produits sont destinés à des personnes physiques ou à des équipements rattachés à une entité morale. Lors de la validation du dossier par l'OCN, ce dernier s'assure que les justificatifs présentés par le demandeur :

- Décrivent explicitement le nom de l'organisation
- Présentent l'identifiant de l'organisation qui doit être un SIREN ou un SIRET valide
- Sont datés de moins de 3 mois
- Font état de la légitimité du demandeur à faire une demande de certificat pour l'organisation concernée.

9.4.3 Validation de l'identité d'un individu

9.4.3.1 Enregistrement d'un porteur

La validation initiale de l'identité d'une demande de certificat se fait lors d'un face-à-face avec l'OCN qui contrôle le dossier de demande de certificats.
Pour les certificats de personnes physique cela se fait avec un OCN de proximité et pour les certificats de cachets, cela se fait avec un OCN central.
Le processus de face à face consiste à s'assurer que l'identité présente sur le justificatif fourni par le demandeur est bien identique à celle fournie dans le formulaire de demande de certificat et que la photo présente sur le justificatif est bien celle du demandeur. L'OCN s'assure également que le justificatif est bien en cours de validité.

9.4.3.2 Enregistrement d'un RCC

L'enregistrement d'un RCC est nécessaire pour une demande de certificat de cachet. Dans ce cadre le dossier de demande :

- Fait explicitement apparaître l'identité du RCC
- Contient un justificatif d'identité du RCC en cours de validité
- Fait état de la légitimité du demandeur à faire une demande de certificat pour l'organisation concernée

9.4.3.3 Enregistrement d'un OCN central

Un OCN central est un personnel de la PNCN. Sa nomination est établie dans le cadre de la gestion des rôles de confiance et une fiche est explicitement produite pour établir l'affectation du rôle à la personne concernée. Cette fiche est signée par le porteur du rôle et par son responsable hiérarchique.

9.4.3.4 Enregistrement d'un OCN

Sa nomination est établie dans le cadre de la gestion des rôles de confiance et une fiche est explicitement produite pour établir l'affectation du rôle à la personne concernée. Cette fiche est signée par le porteur du rôle et par son responsable hiérarchique.

9.4.4 Validation de l'autorité du demandeur

Le dossier de demande de certificat est reçu et vérifié par un OCN. L'OCN s'assure de la légitimité de la demande, sur la base des informations contenues dans le dossier. L'OCN peut au besoin contacter le responsable hiérarchique du demandeur (identifié dans le dossier de demande) pour s'assurer de la légitimité de la demande.

9.5 DEMANDE DE CERTIFICAT

9.5.1 Origine d'une demande de certificat

9.5.1.1 Pour les certificats logiciels

La demande est faite par email par le porteur (ou un intermédiaire).
Le mail peut contenir :

- Directement les informations nécessaires à la production du certificat
- Un fichier contenant une liste d'informations permettant de générer une série de certificats pour plusieurs porteurs

9.5.1.2 Pour les certificats matériels

Une demande de certificat émane du futur porteur, de son supérieur hiérarchique, d'un partenaire ou RCC, qui renseigne le formulaire correspondant.

9.5.2 Processus et responsabilités pour l'établissement d'une demande de certificats

9.5.2.1 Pour les certificats logiciels

Il n'est pas nécessaire de recevoir des justificatifs pour la production des certificats logiciels. L'OCN est donc responsable de s'assurer et de valider les informations qui lui sont transmises pour établir le certificat.

9.5.2.2 Pour les certificats matériels

9.5.2.2.1 Pour les certificats de personnes physiques

Le demandeur d'un certificat doit établir un dossier de demande dans lequel il fournit les justificatifs suivants :

- Le formulaire de demande de certificats. Ce formulaire est signé par le porteur ainsi que par son responsable hiérarchique
- Une photocopie d'un justificatif d'identité en cours de validité (Carte nationale d'identité, passeport ou titre de séjour)
- Un justificatif de moins de 3 mois établissant l'identité de l'organisation d'appartenance du porteur et faisant notamment apparaître explicitement le nom de l'organisation et son identifiant (numéro SIREN/SIRET). Ce justificatif est contre signé par le responsable hiérarchique du porteur
- Le document d'acceptation des CGU paraphées et signées par le porteur

9.5.2.2.2 Pour les certificats de cachet

Le RCC d'un certificat cachet doit établir un dossier de demande dans lequel il fournit les justificatifs suivants :

- Le formulaire de demande de certificats. Ce formulaire est signé par le RCC ainsi que par son responsable hiérarchique. Cela permet de s'assurer que le RCC est bien légitime à faire une demande pour le nom demandé.
- Une photocopie d'un justificatif d'identité en cours de validité (Carte nationale d'identité, passeport ou titre de séjour)
- Un justificatif de moins de 3 mois établissant l'identité de l'organisation d'appartenance du RCC et faisant notamment apparaître explicitement le nom de l'organisation et son identifiant (numéro SIREN/SIRET). Ce justificatif est contre signé par le responsable hiérarchique du porteur
- Les CGU paraphées et signées par le porteur

9.6 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

9.6.1.1 Pour les certificats logiciels

Une fois l'OCN ayant validé les informations à faire apparaître dans le certificat à produire, il réalise les opérations suivantes :

- Connexion sur les interfaces d'enregistrement de la PKI
- Saisie des informations nécessaires à la production du certificat
- Validation dans les interfaces de la production du certificat

9.6.1.2 Pour les certificats matériels

L'identité du porteur ou du RCC, les justificatifs présentés et la connaissance des modalités applicables par le futur porteur sont validés lors d'un face-à-face physique.
Le demandeur se présente auprès de son OCN pour que ce dernier réalise un contrôle de son identité en face à face physique.
L'OCN se charge également de vérifier que le contenu du dossier de demande de certificat est valide et complet. Une fois les étapes de vérifications réalisées, il contresigne la demande de certificat en précisant la date de contrôle du dossier. Cette contre-signature peut se faire de manière manuscrite sur le formulaire de demande ou bien via une signature électronique si l'OCN dispose d'un certificat de signature.

9.6.2 Acceptation ou rejet de la demande

Si le dossier est complet l'OCN se connecte sur les interfaces de gestion des certificats pour créer la demande technique et permettre la production du certificat.
L'OCN informe le porteur en cas de rejet de la demande, en justifiant le rejet. Cette notification de refus est transmise au porteur ou au RCC par courriel ; elle peut être également formulée par l'OCN lors du face-à-face.
Pour les certificats de personnes physiques, si la demande est validée, l'OCN remet au porteur un support QSCD.

9.6.3 Durée d'établissement du certificat

Le certificat est établi soit durant le processus de face-à-face avec l'OCN soit en autonomie par le porteur à l'aide de son support cryptographique et de son code d'activation.
Si la demande est validée, le porteur repart de ce processus avec son support cryptographique prêt à recevoir le certificat ou contenant déjà le certificat établi.

9.7 DELIVRANCE DU CERTIFICAT

L'OCN dispose des outils permettant de faire le retrait du certificat avec le QSCD remis au porteur. Il réalise les étapes en sa présence et lui fait saisir le code d'activation de son QSCD.
La remise et l'activation du QSCD sont formalisées dans une charte de remise et d'utilisation du QSCD signée par le porteur et contresignée par l'OCN. Cette charte est datée.
Les QSCD mis à la disposition des porteurs sont évalués EAL 4+ et qualifiés par l'ANSSI. La clé privée est activée à l'aide d'un code PIN personnel et connu exclusivement du porteur.

9.8 ACCEPTATION DU CERTIFICAT

Le certificat ou le cachet est élaboré en ligne, et transmis lors de la phase d'initialisation du QSCD. Le porteur accepte explicitement son certificat en signant la charte de remise et d'utilisation du QSCD.
Le porteur peut accepter ou refuser le certificat lors de cette phase. Le certificat est présenté visuellement à l'utilisateur.
Si le certificat est refusé par le porteur ou le RCC, l'OCN procède alors à la révocation immédiate du certificat concerné.

10 MODALITES DE RENOUVELLEMENT DE CLES

Un nouveau certificat ne peut pas être fourni au porteur sans renouvellement du bi-clé tant que le QSCD est toujours dans sa phase de validité.
Le porteur devra procéder comme pour une demande initiale (cf. paragraphe 9.5).

11 MODALITE DE REVOCATION

Il existe deux modes au travers desquels peut être effectuée une demande de révocation : révocation standard ou révocation d'urgence.
La révocation standard est effectuée par un OCN. L'OCN s'assure de la légitimité de la demande de révocation et peut de sa propre décision valider la demande de révocation.
La révocation d'urgence peut être à l'initiative du porteur du certificat ou du RCC. Elle peut être effectuée par Internet (voir 3.2). Le porteur ou RCC se connecte directement sur les interfaces de révocation mises à disposition par l'AC.
L'identification du porteur ou RCC et la validation de la demande sont contrôlées par la fourniture, par le porteur, du code de révocation lié au certificat concerné. Ce code a été envoyé lors de la demande de révocation sur l'adresse mail du porteur communiquée lors de la demande de certificat. Une fois le code entré, le certificat est révoqué.
Seul le RCC ou un OCN peut révoquer son certificat.
La révocation par le RCC nécessite l'authentification du RCC.

11.1 CAUSES POSSIBLES D'UNE REVOCATION

Les causes de révocation sont les suivantes :

- Obsolescence des informations figurant dans le certificat
- Création d'un nouveau certificat (avec nouvelles bi-clés) par le porteur avant l'expiration de son certificat précédent
- Décision du porteur ou du RCC
- Erreur dans le dossier de demande de certificat
- Refus du certificat par le porteur ou le RCC durant la phase de remise
- Destruction, altération du QSCD ou de ses fonctions
- Départ du porteur de certificat
- Départ du RCC sans transfert vers un nouveau RCC
- Décision suite à un échec de contrôle de conformité remonté par l'audit interne
- Compromission, suspicion de compromission, perte ou vol de clé privée
- Fin programmée d'utilisation de l'algorithme de condensation mis en œuvre
- Révocation de l'AC SIGNATURE
- Cessation d'activité de l'AC PNCN

11.2 ORIGINE D'UNE DEMANDE DE REVOCATION

Les personnes pouvant demander une révocation sont les suivantes :

- Le porteur ou le RCC au nom duquel le certificat a été émis
- Le responsable hiérarchique du porteur ou du RCC
- L'OCN de proximité pour l'ensemble des porteurs qui lui sont rattachés
- L'OCN central sur l'ensemble des certificats finaux
- Le responsable de l'AC

11.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

L'OCN se connecte sur les interfaces de gestion des certificats. Il recherche ensuite le certificat concerné en utilisant les filtres de recherche du certificat, et notamment en se basant sur le contenu du champ « serialNumber » du « DN » qui contient les informations relatives à l'adresse email du porteur ou du RCC. Si ce dernier dispose de plusieurs certificats actifs, l'OCN identifie via le numéro de série du certificat (si connu par le porteur) ou via les keyUsage le certificat concerné. Une fois le certificat retrouvé, l'OCN déclenche la révocation du certificat en précisant les raisons de la révocation. Cette information est portée dans un champ commentaire et ne sera pas présent dans le contenu de la LCR.

11.4 DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

La demande de révocation est formulée au plus tôt dès lors que le porteur ou le RCC ou son responsable a connaissance d'une cause effective de révocation.

11.5 DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

Le délai maximum de traitement est de 24 heures.

12 LIMITE D'USAGE

12.1 USAGE DE LA BI-CLE ET DU CERTIFICAT

12.1.1 Signature électronique

L'utilisation de la clé privée par le porteur est limitée à la signature de documents. Cet usage est indiqué explicitement dans les extensions du certificat qui présente le keyUsage « contentCommitment ».

12.1.1.1 Bi-clés et certificats de signature qcp-n-qscd

L'utilisation de la clé privée du porteur et du certificat associé est limitée à la signature qualifiée.

12.1.1.2 Bi-clés et certificats de signature qcp-n

L'utilisation de la clé privée du porteur et du certificat associé est limitée à la signature avancée.

12.1.2 Cachet électronique

L'utilisation de la clé privée d'un cachet se fait directement par l'équipement concerné. Après la délivrance du certificat, le RCC est en charge de s'assurer que le certificat de cachet est bien mis en œuvre sur le bon équipement.
L'usage est indiqué explicitement dans les extensions du certificat qui présente le keyUsage « digitalSignature ».
Bi-clés et certificats de cachet qcp-l : L'utilisation de la clé privée et du certificat de cachet associé est limitée au cachet avancé

12.2 UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR L'UTILISATEUR DU CERTIFICAT

L'utilisation du certificat est limitée à la vérification des signatures ou des cachets apposés dans le cadre des applications de dématérialisation du MEN.

12.3 DUREE DE VIE DES BI-CLES ET DES CERTIFICATS

Les clés de signature et les certificats de l'AC ont une durée de vie de 20 ans
Les clés de signature et les certificats des porteurs et les certificats de cachet ont une durée de vie de 3 ans.
Les clés de signature et les certificats éphémères ont une durée de vie de 20 minutes.

13 MODALITES DE VERIFICATION DES CERTIFICATS

13.1 EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

Les applications du MEN souhaitant utiliser les certificats couverts par la PC doivent :

- Recourir au service OCSP,

Ou bien

- S'assurer que :
  - Le certificat final est bien émis par la bonne chaîne d'AC
  - Le certificat final n'est pas révoqué en récupérant le statut de la LCR
  - Le certificat final n'est pas expiré

13.2 EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

Dans le cadre de la révocation d'un certificat d'AC, le C2SC fera publier sur le site de publication une information claire de la compromission de la clé privée. L'AC indiquera sur son site les impacts et les précautions à prendre en la matière.

13.3 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

13.3.1 Caractéristiques opérationnelles

Les LCR sont au format v2, publiées sur le site internet identifié au paragraphe 8.1.

13.3.2 Disponibilité de la fonction

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

13.4 FREQUENCE D'ETABLISSEMENT DES LCR

Les LCR sont émises à minima toutes les 24h.

13.5 DELAI MAXIMUM DE PUBLICATION D'UNE LCR

La publication d'une LCR se fait dans un délai maximum de 30 minutes après sa génération.

13.6 DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS

Les systèmes de révocation et de vérification ont un taux de disponibilité d'au moins 99 pour cent, et sont disponibles 24 heures sur 24. En cas de défaillance du système, l'OSC s'engage à rétablir le système sous 24h.
Ces services bénéficient d'une redondance et d'un plan de reprise d'activité qui permet d'assurer leur disponibilité.

13.7 FIN D'ABONNEMENT

En cas de fin d'activité de l'AC, l'ensemble des certificats émis par la chaîne d'AC correspondante sont révoqués.

13.8 SEQUESTRE DE CLE ET RECOUVREMENT

Il n'est pas procédé à un séquestre de clé.

14 PROTECTION DES DONNEES PERSONNELLES

14.1 POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

Des mesures techniques, procédurales et organisationnelles sont mises en place pour garantir la protection des données personnelles recueillies lors de l'enregistrement. Un registre des données personnelles couvrant le périmètre de la PNCN est établi et tenu à jour. Le responsable des services de l'AC est en charge d'établir ce registre.

14.2 INFORMATIONS A CARACTERE PERSONNEL

Les informations à caractère personnel sont les suivantes :

- Les causes de révocation qui restent confidentielles et ne sont pas publiées ; elles ne sont accessibles qu'au porteur, uniquement sur demande écrite et authentifiée auprès de l'autorité de certification. Le porteur peut adresser une demande par email datée et signée, en utilisant le point de contact identifié au paragraphe 3.2, en mentionnant les éléments d'identification suivants : nom, prénom, adresse email ;
- Les informations d'enregistrement ;
- Le contenu des certificats.

14.3 RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

Conformément au Règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (« RGPD ») et à la règlementation française en vigueur, les traitements de l'AC sont inscrits au registre des traitements et font l'objet de mesures de sécurité techniques et organisationnelles appropriées afin de garantir la conformité à la législation.
L'AC reconnaît avoir procédé ou bien avoir fait procéder aux formalités déclaratives qui leur incombent au titre de la PC et des traitements de données à caractère personnel qui seraient réalisés.

14.4 NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

Conformément aux législations et réglementations en vigueur, en particulier sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.
Le futur porteur a notification d'utilisation des données personnelles [R1], et donne son consentement lors de la phase d'enregistrement. Le porteur peut avoir accès aux informations d'enregistrement.

14.5 CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINISTRATIVES

Les enregistrements peuvent être mis à disposition en cas de besoin pour servir de preuve à la certification en justice.

15 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

15.1 AUTORITES DE CERTIFICATION

Au titre des PC, et pour le domaine qu'elles couvrent, l'AC garantit le respect des engagements décrits dans le présent document et dans l'ensemble des CGU.
Sauf à démontrer qu'elle n'a commis aucune faute intentionnelle ou de négligence, l'AC est responsable de tout préjudice causé à toute personne physique ou morale qui s'est fiée raisonnablement aux certificats délivrés dans chacun des cas suivants :

- Les informations contenues dans le certificat ne correspondent pas aux informations fournies lors de l'enregistrement
- La délivrance du certificat n'a pas donné lieu à vérification de possession de la clé privée correspondante par le porteur
- L'AC ou l'OSC n'a pas fait procéder à l'enregistrement de la révocation d'un certificat, et publié cette information conformément à ses engagements.

Enfin, l'AC engage sa responsabilité en cas de faute ou de négligence dans les précautions à prendre en termes de confidentialité des données personnelles qui lui sont confiées par les porteurs.

15.2 PORTEURS DE CERTIFICATS

Le porteur a le devoir de :

- Communiquer des informations exactes et à jour lors de sa demande de certificat
- Protéger sa clé privée par des moyens adaptés à son environnement
- Protéger ses données d'activation et les mettre en œuvre
- Protéger l'accès à sa base de certificat
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant
- Informer l'AC de toute modification des informations contenues dans son certificat
- Faire sans délai une demande de révocation auprès de son OCN en cas de perte, de compromission ou de suspicion de compromission de sa clé privée
- Interrompre immédiatement et définitivement l'usage de sa clé privée en cas de compromission

La relation entre l'AC et le porteur est formalisée par un engagement du porteur.

15.2.1 Utilisateurs de certificats

Les utilisateurs des certificats doivent :

- Vérifier l'usage pour lequel le certificat a été émis
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application
- Vérifier la signature du certificat du porteur jusqu'à l'AC PNCN et contrôler la validité des certificats

16 LIMITE DE GARANTIES

L'AC ne pourra pas être tenue pour responsable de tout dommage résultant de réclamation par des tiers, de perte de clientèle, d'arrêt de travail ou de tout autre dommage, notamment indirects ou perte commerciale.

17 LIMITE DE RESPONSABILITE

L'AC n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation.
L'AC ne pourra pas être tenue pour responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation du QSCD, des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.
L'AC décline en particulier sa responsabilité pour tout dommage résultant d'un emploi du QSCD pour un usage autre que ceux prévus.
L'AC décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans le QSCD, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur.

18 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

18.1 TYPE D'EVENEMENT A ENREGISTRER

Les éléments suivants font l'objet de traces d'enregistrement :

- Tous les événements relatifs à la sécurité, en particulier :
  - Les changements de politique de sécurité des systèmes ;
  - Les démarrages et arrêts des systèmes ;
  - Les pannes matérielles et logicielles ;
  - Les tentatives d'accès au système PKI.
  - L'activité des pare-feux et des systèmes de routage réseau ;
- Tous les événements relatifs à l'enregistrement des porteurs, en particulier :
  - Réception d'une demande de certificat (initiale et renouvellement) ;
  - Validation / rejet d'une demande de certificat ;
  - Evénements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
  - Génération des certificats des porteurs ;
  - Publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
  - Réception d'une demande de révocation ;
  - Validation / rejet d'une demande de révocation ;
  - Génération puis publication des LAR et LCR.

Ces journaux permettent d'assurer la traçabilité et l'imputabilité des actions effectuées (horodatage, affectation à l'intervenant).

18.2 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

La période de conservation des journaux d'événement est :

- D'un mois pour les événements systèmes
- Douze mois glissants pour les événements techniques
- Conforme aux obligations légales pour les événements fonctionnels

Il s'agit ici de conservation en ligne, disponible directement sur les systèmes de l'OSC. Des durées plus longues de conservation sont mises en œuvre dans le cadre des processus d'archivage.

19 ARCHIVAGE DES DONNEES

19.1 TYPES DE DONNEES A ARCHIVER

Les données à archiver sont les suivantes :

- Logiciels exécutables et fichiers de configuration
- PC, DPC et CGU
- Certificats, LAR et LCR publiés
- Fiches de postes des rôles de confiance signées
- Dossiers de demande de certificats finaux
- Journaux d'événements

19.2 PERIODE DE CONSERVATION DES ARCHIVES

Le tableau suivant présente les périodes de conservation des archives pour chaque type de donnée

Type de données	Période de conservation
Logiciels	Version n – 1
Configurations des logiciels	Version n – 1
Certificats de l'AC SIGNATURE	7 ans après expiration du certificat
Certificats clients	7 ans après expiration du certificat
LCR	Ad vitam après production d'une dernière LCR complète avant la fin de vie de l'AC
Evènements techniques	1 an
Evènements fonctionnels	7 ans après expiration du certificat
Documentation	10 ans
Dossier d'enregistrement (demandes de certificats)	7 ans après expiration du certificat

20 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Un contrôle de conformité à la PC lors de la mise en œuvre opérationnelle du système, et lors de toute modification significative est effectué à travers un audit interne biannuel.

21 TARIFS

L'AC peut imposer des frais notamment pour :

- L'émission ou le renouvellement des certificats
- La mise à disposition d'un annuaire référençant les certificats

La mise à disposition des LCR n'est jamais facturée.

22 RESPONSABILITE FINANCIERE

22.1 COUVERTURE PAR LES ASSURANCES

Les risques susceptibles d'engager la responsabilité du MEN sont couverts en propre par le Ministère.

22.2 AUTRES RESSOURCES

Le MEN reconnaît disposer d'une garantie financière suffisante spécialement affectée à la couverture des risques financiers sur les activités de l'AC.

22.3 INDEMNITES

Sans objet

23 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

Conformément aux textes législatifs et à la réglementation en vigueur, les certificats émis en vertu de la Politique Certification sont des certificats dont les conditions d'utilisation sont définies par la Politique Certification et par les présentes conditions générales d'utilisation qui définissent les relations entre les différentes parties prenantes.

24 JURIDICTIONS COMPETENTES

Les présentes Conditions Générales d'Utilisation sont soumises au droit français.
Tout litige relatif à la validité, l'interprétation, et/ou l'exécution de les présentes CGU sera soumis aux tribunaux compétents de la cour d'appel de Paris.

25 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

En sus de la règlementation RGPD, l'AC SIGNATURE vise une certification aux normes ETSI 319401, ETSI 319411-1 et pour les profils de certificats qualifiés une certification à la norme ETSI 319411-2.
De plus les profils de certificats qualifiés font l'objet d'une demande de qualification conformément au règlement européen, 910/2014 dit règlement eIDAS [eIDAS].

26 FORCE MAJEURE

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.