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

Plateforme Nationale de Confiance Numérique

Politique de Certification pour les certificats de l'Autorité de Certification Racine

PC AC PNCN – Format RFC 3647

Statut du document : en cours de rédaction
Version : 2.1

PUBLIE

Entrée en vigueur le 19/06/2024

Table des matières

1. INTRODUCTION

1.1. PRESENTATION GENERALE

Le présent document définit l'ensemble des exigences auxquelles le Ministère de l'Education Nationale (MEN) se conforme dans la mise en place et la fourniture de ses prestations de service de certification électronique à destination des agents du ministère et de ses partenaires. La mise en œuvre de ces fonctions se fait à travers la Plateforme Nationale de Confiance Numérique (PNCN).
Les exigences définies dans le présent document constituent une déclinaison des exigences relatives aux prestataires de services de certification en vue de la reconnaissance de leur qualification définie dans le règlement européen [A2], et en particulier des exigences définies dans les documents [A5], [A6], [A8], [A9].
Le MEN s'est positionné comme prestataire de service de certification électronique, en proposant des services supports à la signature électronique de manière à permettre la dématérialisation des processus métiers et plus généralement de sécuriser l'ensemble des échanges.
Pour ce faire, une hiérarchie de certification a été mise en place, qui est présentée dans le paragraphe 1.3. La présente politique de certification définit les exigences relatives à l'AC PNCN, qui est l'AC racine de la chaîne de certification et qui est utilisée pour signer des certificats d'autorités de certification filles. Sa structure est conforme au RFC 3647, [A1]. Il s'agit d'une Autorité de Certification en mode hors-ligne et dont le certificat est auto-signé.

1.2. IDENTIFICATION DU DOCUMENT

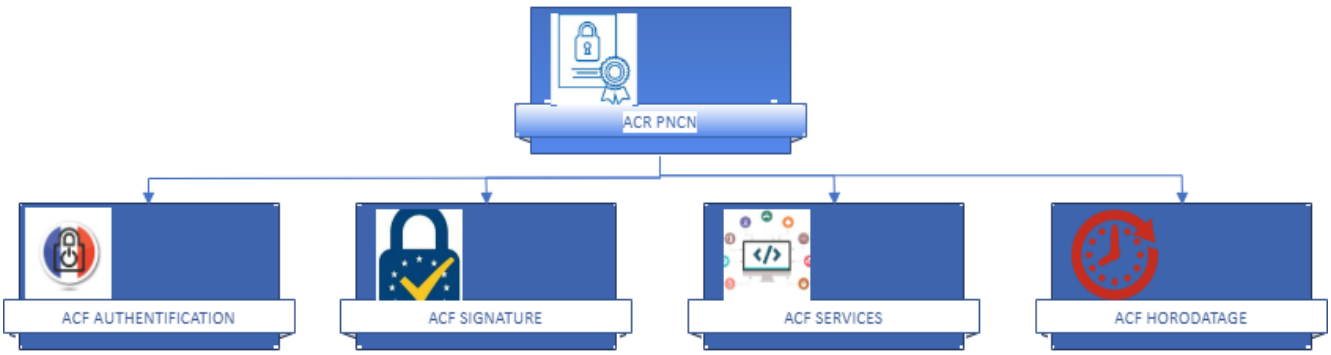
Le numéro d'OID du présent document est 1.2.250.1.535.2.2.2.2.1.1.3.

1.3. ENTITES INTERVENANT DANS L'IGC

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

- Signer les demandes de certificats des certificats des AC Filles
- Signer la Liste des Autorités Révoquées (LAR)

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 à la PNCN en tant qu'Opérateur de Service de Certification (OSC), pour opérer les fonctions de gestion des certificats.

1.3.1. Autorités 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 présente 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 ceux d'Autorités de Certification Filles rattachées à l'Autorité de Certification Racine.

1.3.2. Opérateur 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 publication des informations
- La fonction de gestion des révocations
- La fonction d'information sur l'état des certificats

1.3.3. Autorité d'enregistrement (AE)

Dans le cadre de l'AC PNCN, les activités d'AE sont directement réalisées par l'AC.

1.3.4. Porteurs de certificats

Sans objet, les certificats couverts par cette PC sont des certificats d'Autorités de Certification, il n'y a donc pas de porteurs.

1.3.5. Utilisateurs de certificats

Les certificats couverts par la présente PC sont utilisés dans les applications métiers mises en œuvre par le MEN ou des partenaires. Il s'agit donc d'application métiers ayant des besoins de valider des certificats finaux émis par une des AC filles de la chaîne d'AC portée par l'AC PNCN.

1.4. USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

Les certificats couverts dans la présente PC sont ceux de la hiérarchie portée par l'AC PNCN.

1.4.2. Domaines d'utilisation interdits

En dehors des usages identifiés dans le paragraphe précédent, tous les autres usages ne sont pas couverts par la présente PC.

1.5. GESTION DE LA PC

1.5.1. Entité gérant la PC

La gestion de la PC est de la responsabilité de l'Autorité de Certification. Pour cela La gouvernance est assurée à travers le « Bureau de la sécurité » et son Comité de Suivi des Services de Confiance (C2SC).
Le comité se réunit mensuellement pour traiter des points liés à la PNCN.
Un responsable des aspects SSI du périmètre des Autorités de Certification est identifié.

1.5.2. Point de contact

Toutes questions concernant la présente politique ou la gestion des services de confiance sont à adresser à l'adresse email suivante : service.certification@pncn.education.gouv.fr.

1.5.3. Entité déterminant la conformité d'une DPC avec ce document

Le Pôle National de la Sécurité des Systèmes d'Information est en charge de piloter le contrôle interne. Le périmètre de la PNCN et des services de confiance est intégré à leurs processus d'audit. Sur la base de rapport de contrôle de conformité, le C2SC est en charge de prononcer la conformité de la Déclaration des Pratiques de Certification (DPC) (et des procédures associées) à la Politique de Certification.

1.5.4. Procédures d'approbation de la conformité de la DPC

L'approbation de la conformité à la DPC est formalisée à travers un compte rendu du C2SC. Cette approbation intervient préalablement à la production d'un certificat final par les services concernés par la présente PC.

1.6. DEFINITIONS ET ACRONYMES

1.6.1. Acronymes

AC	**A**utorité de **C**ertification
AE	**A**utorité d'**E**nregistrement
ANSSI	**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation
ARL	**A**uthority **R**evocation **L**ist = LAR en français
C2SC	**C**omité de **S**uivi des **S**ervices de **C**onfiance
COSSIM	**C**entre **O**pérationnel de **S**écurité des **S**ystèmes d'**I**nformation Ministériel
CRL	**C**ertificate **R**evocation **L**ist = LCR en français
DN	**D**istinguished **N**ame
DPC	**D**éclaration de **P**ratiques de **C**ertification
ETSI	Institut européen des normes de télécommunication (**E**uropean **T**elecommunications **S**tandards **I**nstitute)
HTTP	**H**yper**T**ext **T**ransfer **P**rotocol
IGC	**I**nfrastructure de **G**estion de **C**lés
ISO	**I**nternational **O**rganization for **S**tandardization
LAR	**L**iste des **A**utorités **R**évoquées
LCR	**L**iste des **C**ertificats **R**évoqués
MEN	**M**inistère de l'**E**ducation **N**ationale
OID	Identifiant d'objet (**O**bject **ID**entifier)
OSC	**O**pérateur de **S**ervice de **C**ertification
OCSP	**O**n-line **C**ertificate **S**tatus **P**rotocol
PC	**P**olitique de **C**ertification
PNCN	**P**lateforme **N**ationale de **C**onfiance **N**umérique
PSCE	**P**restataire de **S**ervice de **C**ertification **E**lectronique
PSCo	**P**restataire de **S**ervice de **Co**nfiance
RFC	**R**equest **F**or **C**omments
RGS	**R**éférentiel **G**énéral de **S**écurité
SIEM	**S**ecurity **I**nformation **E**vent **M**anagement
SIREN	**S**ystème d'**I**dentification du **R**épertoire des **EN**treprises
UTC	**U**niversal **T**ime **C**oordinated

1.6.2. Définitions

Audit : Contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures

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

Autorité d'enregistrement (AE) : Entité responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face à face. L'AE effectue en outre, les opérations de demandes de certificat

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

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

2.1. 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%.

2.2. INFORMATIONS DEVANT ETRE PUBLIEES

Les informations publiées sont les suivantes :

- La présente politique de certification
- La liste des Autorités Révoquées (LAR) pour les certificats d'AC
- Les certificats de l'AC PNCN en cours de validité
- Le condensat SH256 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

Le document PC est publié :

- Au format PDF/A
- En français.

2.3. DELAIS ET FREQUENCES DE PUBLICATION

Les politiques de certification sont remises à jour 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 LAR, dans un délai de 72 heures.
La fréquence de publication des LAR est compatible avec un délai maximal de 24 heures entre la prise en compte d'une demande de révocation et sa publication. Les LAR sont publiées tous les mois.

2.4. CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

Les demandes de publication sont faites par l'AC à travers des demandes tracées dans des outils internes de suivi de ticket. Opérationnellement la demande est traitée par l'OSC puis contrôlée pour bonne application par l'AC.
La publication peut se faire manuellement par un administrateur disposant des habilitations systèmes nécessaires (publication de documents liés aux activités de l'AC) ou bien de manière automatique par des scripts programmés au niveau du serveur de publication (publication des nouvelles LAR).
Le processus de publication de la LAR permet de s'assurer de :

- L'intégrité de la LAR
- Du contenu de la LAR
- Du séquençage de la LAR

Les personnes disposant d'un rôle d'administrateur sur le serveur de publication s'authentifient nominativement sur le serveur via un mécanisme d'authentification forte.
L'accès en lecture est disponible pour tous.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. NOMMAGE

3.1.1. Types de noms

Les noms utilisés dans un certificat sont décrits selon la norme ISO/IEC 9594 (distinguished names), [A3], chaque titulaire ayant un nom distinct (DN).

3.1.2. Nécessité d'utilisation de noms explicites

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

- 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 »
- Le nom de l'AC dans le champ « commonName »

3.1.3. Anonymisation ou pseudonymisation

Sans objet

3.1.4. Règles d'interprétation des différentes formes de noms

Les informations portées dans un certificat d'AC sont validées préalablement à sa génération par le C2SC. Le comité est garant de la légitimité à utiliser des noms d'AC sous le périmètre du MEN.

3.1.5. Unicité des noms

La génération d'un certificat d'AC nécessite un processus organisationnel préalable. Un comité est prévu pour valider le nom d'une nouvelle AC, ce processus s'assure que le nom est bien unique dans le temps.

3.1.6. Identification, authentification et rôle des marques déposées

Pour les marques, dénominations sociales ou autres signes distinctifs, l'AC n'effectue aucune recherche d'antériorité ou autre vérification ; il appartient au demandeur ou au titulaire de vérifier que la dénomination demandée ne porte pas atteinte à des droits de propriété de tiers.

3.2. VALIDATION INITIALE DE L'IDENTITE

3.2.1. Méthode pour prouver la possession de la clé privée

Les clés privées ne sont pas extraites en dehors du domaine de sécurité du matériel cryptographique utilisé pour les générer et les stocker. Les clés privées de l'AC ne signent que des demandes de certificats pour des AC Filles où les clés privées sont générées dans une cérémonie des clés en présence d'un huissier, sous la responsabilité de l'AC.

3.2.2. Validation de l'identité d'un organisme

Lors de la validation de la demande par le C2SC, 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.

3.2.3. Informations non vérifiées

Sans objet

3.2.4. Validation de l'autorité du demandeur

Le demandeur est présent lors de la cérémonie des clés.
A cette occasion, le maître de cérémonie demande aux personnes présentes de fournir les pièces suivantes :

- Pièce justificative de l'identité (carte d'identité, passeport ou permis de conduire) ;
- Le formulaire de demande de création de l'AC Fille concernée, signé, et détaillant les caractéristiques nécessaires à la génération de ce nouveau certificat d'AC (nom de l'AC, caractéristiques techniques), contenant :
    - Le nom de l'AC ;
    - Le nom de l'organisation de l'AC et son numéro SIREN ;
    - Le type et taille du bi-clé à créer
    - La durée de vie de l'AC
    - Le type d'usage de la clé : signature de certificat seulement ou signature de certificat et de Liste de d'Autorités Révoquées (LAR).

Le lancement de la cérémonie des clés est lié à la vérification préalable par le maître de cérémonie du formulaire de demande de création de l'AC Fille.
L'ensemble des actions réalisées durant la cérémonie des clés est conservé et archivé dans le procès-verbal de cérémonie.

3.2.5. Certification croisée d'AC

L'AC n'a aucun accord de reconnaissance avec une AC extérieure au domaine de sécurité auquel elle appartient. Les certificats qu'elle émet à travers la présente PC sont à des fins d'utilisation interne au MEN. Si l'AC devait produire des certificats pour d'autres entités que celles du MEN, le C2SC établirait formellement une organisation au sein de ces autres entités pour assurer que les processus de gestion des certificats sont aux mêmes niveaux d'exigences que ceux décrits dans cette PC.
Si une autre AC formule une demande d'accord, ou si les responsables de l'AC PNCN émettent le besoin de mettre en place un accord de reconnaissance avec une autre AC, le C2SC diligentera une série d'investigations (audits / analyse de risques) pour déterminer si l'AC à reconnaître émet bien des certificats de même qualité, avec le même niveau de sécurité, que ceux de la présente AC.
Notamment, l'AC PNCN pourra attendre des AC demandant un accord de certification de respecter les formats des certificats suivant la norme [A8], [A9].

3.3. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DE CLES

Un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la clé privée.
Le renouvellement se traduit alors par une nouvelle demande de certificat et bénéficie des mêmes procédures que pour une demande initiale.

3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE REVOCATION

La demande de révocation de clé pour une AC Fille signée par l'AC PNCN ne peut émaner que d'une personne autorisée, et est validée formellement avant prise en compte par le C2SC.
Le certificat de l'AC PNCN étant un certificat auto-signé, il ne peut pas être révoqué.
En cas de compromission de la clé privée correspondante au certificat de l'AC PNCN, l'AC publiera une information sur le site identifié au paragraphe 2. Cela permet à tout porteur ou à toute application utilisatrice d'être informé de cette compromission.
La révocation est effectuée par une personne habilitée de la PNCN en utilisant les interfaces et les outils mis à disposition de l'AC.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. DEMANDE DE CERTIFICAT

4.1.1. Origine d'une demande de certificat

Une demande de certificat émane de la personne autorisée par l'organisation, présente lors de la cérémonie des clés. La demande est nécessairement validée par le C2SC préalablement à son traitement.

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

L'établissement d'une demande de certificat s'effectue selon une procédure de cérémonie de clés. Les opérations techniques se font dans une salle protégée et prévue à cet effet.

4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Les clés de l'AC PNCN ne sont mises en œuvre que dans le cadre d'une cérémonie de clés soit pour :

- La signature d'une demande de certificat pour un certificat d'AC Fille
- La signature d'une nouvelle ARL

En dehors de ces phases, les clés de l'AC PNCN restent hors ligne.
La génération des clés d'AC se fait lors de la phase de cérémonie des clés en présence d'un représentant de l'AC, des administrateurs techniques et des porteurs de secrets. Cette génération se fait dans un environnement dédié à l'AC PNCN.
Cette cérémonie des clés est constatée par un huissier et des témoins sur la base d'un script de cérémonie des clés établi au préalable.

4.2.2. Acceptation ou rejet de la demande

Toutes les demandes de certificat sont acceptées ou rejetées avant la signature de cette demande par l'AC PNCN. Cette acceptation ou se rejet sont prononcés par le C2SC au travers un compte rendu de comité.

4.2.3. Durée d'établissement du certificat

Les certificats des AC Filles signés par l'AC PNCN sont générés durant la cérémonie des clés et installés dans un temps le plus court possible à l'issue de la cérémonie.

4.3. DELIVRANCE DU CERTIFICAT

4.3.1. Actions de l'AC concernant la délivrance du certificat

La génération des bi-clés est consignée lors de la cérémonie des clés. Cette génération se fait dans l'environnement dédié à l'AC PNCN. Cela consiste à faire signer par la bi-clé de l'AC PNCN la demande de certificat de l'AC Fille. Cette demande de certificat est transmise à l'AC PNCN via un support physique dédié à cette opération.

4.3.2. Notification par l'AC de la délivrance du certificat

Le responsable de l'AC est présent lors de la cérémonie des clés.

4.4. ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

L'acceptation du certificat signé par l'AC PNCN est consignée sur le procès-verbal de la cérémonie des clés. Le procès-verbal est contresigné par l'huissier présent et remis au responsable de l'AC PNCN.

4.4.2. Publication du certificat

Le certificat de l'AC PNCN et des certificats signés par cette AC sont publiés sur le point de publication indiqué au paragraphe 2.

4.4.3. Notification par l'AC aux autres entités de la délivrance du certificat

Sans objet.

4.5. USAGE DE LA BI-CLE ET DU CERTIFICAT

4.5.1. Utilisation de la clé privée et du certificat

La clé privée est utilisée pour :

- Signer des certificats d'AC Filles ;
- Signer la liste des autorités révoquées.

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

L'utilisation de la clé publique et du certificat est limitée au contrôle des certificats gérés par les AC Filles, et à la validation des LAR.

4.6. RENOUVELLEMENT D'UN CERTIFICAT

La notion de renouvellement de certificat, au sens RFC 3647, [A1], correspondant à la seule modification des dates de validité, n'est pas retenue. Seule la délivrance d'un nouveau certificat suite à changement de la bi-clé est autorisée.

4.6.1. Causes possibles de renouvellement d'un certificat

Sans objet

4.6.2. Origine d'une demande de renouvellement

Sans objet

4.6.3. Procédure de traitement d'une demande de renouvellement

Sans objet

4.6.4. Notification de l'établissement du nouveau certificat

Sans objet

4.6.5. Démarche d'acceptation du nouveau certificat

Sans objet

4.6.6. Publication du nouveau certificat

Sans objet

4.6.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet

4.7. DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI-CLE

4.7.1. Cause possible de changement de bi-clé

La bi-clé est changée suite à une révocation ou bien suite à la fin de vie du certificat précédemment délivré.

4.7.2. Origine d'une demande de nouveau certificat

Dans tous les cas, la procédure de demande de nouveau certificat est identique à la procédure de demande initiale.

4.7.3. Procédure de traitement d'une demande de nouveau certificat

Identique à la demande initiale.

4.7.4. Notification de l'établissement du nouveau certificat

Identique à la demande initiale.

4.7.5. Démarche d'acceptation du nouveau certificat

Identique à la demande initiale.

4.7.6. Publication du nouveau certificat

Identique à la demande initiale.

4.7.7. Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Identique à la demande initiale.

4.8. MODIFICATION DU CERTIFICAT

Les modifications de certificats ne sont pas autorisées.

4.8.1. Cause possible de modification d'un certificat

Sans objet

4.8.2. Origine d'une demande de modification de certificat

Sans objet

4.8.3. Procédure de traitement d'une demande de modification de certificat

Sans objet

4.8.4. Notification de l'établissement du certificat modifié

Sans objet

4.8.5. Démarche d'acceptation du certificat modifié

Sans objet

4.8.6. Publication du certificat modifié

Sans objet

4.8.7. Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet

4.9. REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1. Causes possibles d'une révocation

4.9.1.1. Certificats finaux

Les causes de révocation sont les suivantes :

- Obsolescence des informations figurant dans le certificat
- Compromission, suspicion de compromission, perte ou vol de clé privée
- Compromissions ou dépréciation d'algorithme
- Cessation de l'activité de l'AC
- Décision suite à un échec de contrôle de conformité
- Compromission de l'AC PNCN

4.9.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation sont les suivantes :

- Le responsable de l'AC
- Le C2SC

4.9.3. Procédure de traitement d'une demande de révocation

La demande de révocation est validée par le C2SC et elle est formalisé à travers un compte rendu du comité.
La révocation d'un certificat d'AC se fait dans le cadre d'une cérémonie des clés. La clé privée de l'AC PNCN devant être mise en œuvre dans ce cadre, le quorum des porteurs de secrets est nécessaire. A l'issue de la révocation du certificat d'AC, les LAR pré-générées sont détruites et de nouvelles LAR sont produites. La LAR active est alors mise en ligne.

4.9.4. Délai accordé pour formuler la demande de révocation

La demande de révocation doit être formulée au plus tôt dès la connaissance d'une cause effective de révocation.

4.9.5. Délai de traitement par l'AC d'une demande de révocation

L'AC s'engage à traiter la demande de révocation d'un certificat d'AC dans les meilleurs délais après réception de la demande avec un délai maximal de 72 heures.

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

Les applications du MEN souhaitant utiliser les certificats couverts par la présente PC doivent s'assurer que :

- Le certificat d'AC est bien émis par l'AC PNCN
- Le certificat d'AC n'est pas révoqué en récupérant le statut de la LAR
- Le certificat d'AC n'est pas expiré

4.9.7. Fréquence d'établissement des LAR

Un ensemble de 12 LAR est généré en cérémonie de clés et ces LAR sont signées par l'AC PNCN.
Chaque LAR a :

- Une durée de 45 jours
- Une période de renouvellement de 15 jours.

4.9.8. Délai maximum de publication d'une LCR

La LAR suivante est publiée au maximum 15 jours après la fin du mois de validité de la précédente. En cas de révocation d'un certificat d'AC, la nouvelle LAR valide est publiée immédiatement.

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

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

Voir 4.9.6.

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

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.

4.9.13. Causes possibles d'une suspension

La suspension de certificat n'est pas prévue.

4.9.14. Origine d'une demande de suspension

Sans objet

4.9.15. Procédure de traitement d'une demande de suspension

Sans objet

4.9.16. Limites de la période de suspension d'un certificat

Sans objet

4.10. FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.10.1. Caractéristiques opérationnelles

Les LAR sont au format v2, publiées sur le site internet identifié au paragraphe 2.1.

4.10.2. Disponibilité de la fonction

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

4.10.3. Dispositifs optionnels

Sans objet.

4.11. 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.

4.12. Sequestre de cle et recouvrement

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

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Sans objet

4.12.2. Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet

5. MESURES DE SECURITE NON TECHNIQUES

5.1. Mesures de securite physique

5.1.1. Situation géographique et construction des sites

Les sites d'hébergement sont situés en France et leur exposition géographique couvre par des mesures particulières les risques de type tremblement de terre, explosion, risque volcanique ou crue.

5.1.2. Accès physique

L'accès physique aux fonctions de génération des certificats, génération des éléments secrets, gestion des révocations et/ou toutes fonctions opérées par l'OSC, est strictement limité aux seules personnes nominativement autorisées.
L'accès physique aux composantes de l'IGC supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants.
La traçabilité des accès est assurée.
En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.
Des mesures de sécurité physique sont également mises en place pour limiter les accès aux supports sensibles (supports de clés, dossier d'enregistrement, documents d'applications).

5.1.3. Alimentation électrique et climatisation

Des mesures de secours sont mises en œuvre par l'OSC de manière à ce qu'une interruption de service d'alimentation électrique, ou une défaillance de climatisation ne portent pas atteinte aux engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier).
Les composants techniques de l'IGC sont redondés sur plusieurs sites.

5.1.4. Exposition aux dégâts des eaux

La définition du périmètre de sécurité prend en considération les risques inhérents aux dégâts des eaux. Des moyens de protection sont mis en œuvre pour parer les risques résiduels (rupture de canalisation par exemple).

5.1.5. Prévention et protection incendie

Les moyens de prévention et de lutte contre l'incendie permettent de respecter les engagements pris par l'AC en matière de disponibilité (gestion des révocations et informations relatives à l'état des certificats en particulier), et de pérennité de l'archivage.

5.1.6. Conservation des supports

Les moyens de conservation des supports permettent de respecter les engagements pris par l'AC en matière de restitution et de pérennité de l'archivage.

5.1.7. Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction, ou peuvent être réutilisés dans un contexte opérationnel identique à un même niveau de sensibilité.

5.1.8. Sauvegarde hors site

Afin de permettre une reprise après incident conforme aux engagements pris par l'AC, l'OSC met en place des sauvegardes hors site des informations et fonctions critiques. La confidentialité des informations, et l'intégrité des applications sauvegardées sont garantie de manière homogène sur le site opérationnel et sur le site de sauvegarde.
Cela concerne en particulier les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.2. MESURES DE SECURITE PROCEDURALES

5.2.1. Rôles de confiance

L'Autorité du service est l'autorité à laquelle les utilisateurs et clients font confiance pour la fourniture du service de confiance. Ce terme désigne l'entité responsable des services fournis. Dans le cadre de la PNCN, la responsabilité du service de confiance est assurée par le sous-directeur de la DNE – SOCLE 4 à travers la Direction du Numérique de l'Education Nationale (DNE).
La gouvernance est assurée à travers le « Bureau de la sécurité » SOCLE 4 et son C2SC. Le comité se réunit mensuellement pour traiter des points liés à la PNCN.
La structure organisationnelle du service de confiance se décline en différentes fonctions :

- Au niveau du service de confiance (Autorité de Certification) :
    - Représentant légal du service ;
    - Responsable de l'autorité de certification ;
    - Responsable de la sécurité ;
    - Responsable des Officiers de Confiance Numérique ;
    - Porteurs de secrets (titulaire d'une partie des secrets générés lors de la cérémonie des clés).
- Au niveau de l'Opérateur de Services de Confiance (rôles définis au niveau des équipes de la PNCN) :
    - Responsable PNCN ;
    - Responsable Opérationnel de la Sécurité ;
    - Administrateurs systèmes ;
    - Ingénieurs Sécurité ;
    - Administrateurs HSM ;
    - Exploitants et superviseurs ;
    - Auditeur Système ;
- Au niveau de l'organisation transverse du service :
    - Responsable de l'audit interne des composantes de la PNCN ;
    - Responsable des problématiques juridiques de la PNCN ;

5.2.2. Nombre de personne requis par tâche

Les différentes entités du service de confiance s'organisent pour assurer la disponibilité de leurs personnels en fonction des tâches qui leurs sont dédiées.
La reconstruction du secret de l'AC nécessite le regroupement de 3 porteurs de secrets parmi 5 chacune possédant une partie du secret.

5.2.3. Identification et authentification pour chaque rôle

Des mesures d'identification et d'authentification sont mises en place afin de supporter la mise en œuvre de la politique de contrôle d'accès et la traçabilité des opérations ; la politique de contrôle d'accès limite l'accès aux seules personnes habilitées à réaliser les opérations d'administration et de génération de clés sur l'infrastructure de confiance.
Les rôles attribués sont notifiés par écrit aux personnes concernées dans la description de poste et sont contresignées par le responsable hiérarchique. Les formulaires d'obtention d'un rôle de confiance permettent d'assurer le suivi de ce rôle, notamment les modifications de postes dans le temps ou le retrait d'un rôle de confiance.

5.2.4. Rôles exigeant une séparation des attributions

De manière générale, les rôles de responsabilités et les rôles opérationnels sont séparés.
Au sein de l'OSC, les rôles d'administrateurs et les rôles d'exploitants/superviseurs ne sont pas cumulés.
Enfin le rôle d'auditeur système ne fait l'objet d'aucun cumul.

5.3. MESURES DE SECURITE VIS A VIS DU PERSONNEL

5.3.1. Qualifications, compétences, et habilitations requises

Tout intervenant amené à occuper un rôle de confiance est soumis à une clause de confidentialité et de non-conflit d'intérêts, gérée par la PNCN. En outre les intervenants disposant d'un rôle de confiance attestent sur l'honneur n'avoir commis aucun délit en matière de cybercriminalité.
L'OSC s'assure que les attributions des personnels opérant sur des postes sensibles correspondent à leurs compétences professionnelles. Notamment les personnels de l'OSC suivent des formations au moins annuellement sur les menaces informatiques et les pratiques de sécurité du système d'information.
Le personnel d'encadrement possède l'expertise appropriée, et est familier des procédures de sécurité.
Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (description de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2. Procédures de vérification des antécédents

Des procédures de vérification des antécédents sont mises en place pour les personnes appelées à occuper un rôle de confiance. Notamment il est demandé au futur porteur d'un rôle de confiance lors d'une prise d'un rôle de confiance de fournir l'extrait n°3 du casier judiciaire. Pour chaque porteur d'un rôle de confiance, une revue de l'extrait n°3 du casier judiciaire est effectuée au moins une fois tous les 3 ans.

5.3.3. Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Cela concerne essentiellement le personnel de l'OSC opérant sur les composantes de l'IGC, mais également les OCN pour l'utilisation des interfaces de gestion des certificats.

5.3.4. Exigences en matière de formation continue et fréquences des formations

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.
Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

5.3.5. Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6. Sanctions en cas d'actions non autorisées

Les sanctions en cas d'actions non autorisées sont énoncées dans la définition de poste ou la charte de sécurité du personnel pour les rôles sensibles tenus par le personnel de l'OSC et de l'AC.

5.3.7. Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis des prestataires externes sont contractualisées.

5.3.8. Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant. Les personnes appelées à occuper un rôle opérationnel dans le service de confiance disposent des procédures correspondantes.

5.4. PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

5.4.1. Type d'événement à 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 la gestion des certificats d'AC, 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, ...) ;
  - 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.

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

5.4.2. Fréquence de traitement des journaux d'événements

Toutes les actions sont formalisées dans un procès-verbal de cérémonie des clés. Ce Procès-verbal est signé par le responsable de l'AC.

5.4.3. Période de conservation des journaux d'événements

Les journaux techniques sont conservés directement dans l'environnement utilisé pour réaliser les cérémonies des clés, cet environnement étant éteint en dehors d'une cérémonie des clés.

5.4.4. Protection des journaux d'événements

Les journaux d'événements sont accessibles uniquement au personnel autorisé de l'OSC. Ils ne sont pas modifiables de manière non autorisée ; des alarmes sont remontées en cas de modification des journaux, ou des paramètres définissant le contenu des journaux.

5.4.5. Procédure de sauvegarde des journaux d'événements

Les éléments de journalisation sont sauvegardés à l'issue d'une cérémonie des clés.

5.4.6. Système de collecte des journaux d'événements

Sans objet.

5.4.7. Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet

5.4.8. Evaluation des vulnérabilités

L'environnement n'est pas connecté sur le réseau durant sa mise en route en cérémonie des clés et est conservé éteint en dehors des cérémonies.

5.5. ARCHIVAGE DES DONNEES

5.5.1. Types de données à archiver

Les données à archiver sont les suivantes :

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

5.5.2. Période 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 des AC	7 ans après expiration du certificat
LAR	Ad vitam après production d'une dernière LAR complète avant la fin de vie de l'AC
Evènements techniques	Ad vitam
Evènements fonctionnels	Ad vitam
Documentation	10 ans après expiration du certificat
Dossier d'enregistrement (demandes de certificats)	7 ans après expiration du certificat

5.5.3. Protection des archives

Quel que soit leur support, les archives sont protégées en intégrité, et ne sont accessibles qu'aux personnes autorisées. Ces archives sont lisibles et exploitables sur l'ensemble de leur cycle de vie.
L'OSC met en œuvre les moyens nécessaires pour garantir la conservation des archives sur une période conforme aux exigences légales en matière de fourniture d'éléments de preuves.

5.5.4. Procédure de sauvegarde des archives

Les archives sont sauvegardées de manière sécurisée. Les moyens mis en œuvre pour réaliser la sauvegarde garantissent que les éléments ne peuvent pas être supprimés ou détruits facilement.

5.5.5. Exigences d'horodatage des données

L'horodatage des données des événements journalisés est synchrone en dehors des opérations hors ligne. Pour cela, les composants de l'environnement utilisé durant les cérémonies des clés est mis à jour manuellement, avant démarrage des opérations techniques.

5.5.6. Système de collecte des archives

Sans objet.

5.5.7. Procédure de récupération et de vérification des archives

La récupération et la vérification des archives peuvent être effectuées dans un délai conforme à l'utilisation des certificats délivrés. Un délai de 7 jours ouvrés est nécessaire pour récupérer les archives et les mettre à disposition du demandeur.

5.6. CHANGEMENT DE CLES D'AC

La durée de vie des clés d'AC PNCN est de 20 ans. La durée de vie des certificats d'AC Fille est de 20 ans. L'ensemble de la chaîne d'AC devra être renouvelé :

- A la fin de vie
- Au renouvellement anticipé d'un certificat d'AC Fille

5.7. REPRISE SUITE A COMPROMISSION ET SINISTRE

5.7.1. Procédure de remontée et de traitement des incidents et des compromissions

Des procédures et des moyens de remontée et de traitement des incidents (sensibilisation, formation des personnels, et analyse des différents journaux d'événements) sont mis en œuvre.
Un incident majeur – perte, suspicion de compromission, compromission ou vol de clé privée de gestion des certificats par exemple – est immédiatement signalé à l'AC. La publication de révocation du certificat, si elle s'avère nécessaire, est effectuée dans la plus grande urgence par tout moyen nécessaire.

5.7.2. Procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Un plan de continuité est mis en place permettant de répondre aux exigences de disponibilité des différentes composantes de l'IGC.

5.7.3. Procédures de reprise en cas de compromission de la clé privée d'une composante

La compromission d'une clé d'AC entraîne immédiatement la révocation du certificat correspondant. Les cas de compromission des éléments secrets des autres composantes sont traités dans le plan de continuité d'activité. La révocation en cascade de tous les certificats émis par cette AC est également mise en œuvre. L'AC définit dans ses pratiques les modalités permettant aux tiers de déterminer le statut d'un certificat à un moment donné, la dernière LCR dans ce contexte n'étant plus considérée fiable.
Les éléments ci-après traitent de la compromission d'un algorithme ou d'un paramètre associé, tels que l'algorithme de condensat utilisé dans les certificats ou la longueur de la clé des certificats.
L'AC et plus particulièrement l'OSC se tiennent continuellement informés des cas de compromission des éléments susmentionnés, auprès de groupes d'experts en sécurité des systèmes d'information.
En cas d'information d'une compromission impactant les certificats des AC, l'AC et l'OSC déclenchent une cellule de crise afin de déterminer les actions à mener pour rétablir le service au plus tôt.
Par mesure de précaution, l'AC :

- Demande à l'OSC l'arrêt immédiat des services exploitant les certificats de l'AC PNCN;
- Fait diffuser immédiatement l'information à toutes les parties prenantes par mail (porteurs, OCN, partenaires).

5.7.4. Capacités de continuité d'activité suite à un sinistre

Chaque entité opérant une composante de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements, y compris dans le cas d'incidents majeurs (compromission de clés privées, faiblesse des algorithmes utilisés, …). Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'AC dans les présentes PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.
Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les engagements des présentes PC.
En cas de détection d'un incident de sécurité sur l'infrastructure de confiance, l'AC doit en être informée, et s'engage à informer le COSSIM qui se charge ensuite, pour les incidents liés à la sécurité ou pour toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel, de prévenir l'ANSSI à travers l'adresse suivante : cert-fr.cossi@ssi.gouv.fr
Les composants de la PNCN sont redondés sur plusieurs salles en mode actif/passif. Un sinistre majeur déclenche la bascule des services vers la seconde salle.
En cas de destruction du site d'hébergement, l'AC établit dans le cadre d'une cellule de crise les conditions de continuité de son service de confiance. En fonction des éléments, l'AC pourra considérer :

- Déclencher la fin de vie de ses services de confiance et assurer le transfert des activités de publication vers un tiers
- Reconstruire ses services sur un autre site, cela pouvant passer par la reconstruction de la chaîne d'AC ou bien par la mise en œuvre d'une nouvelle chaîne d'AC.

5.8. Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC, ou la totalité de l'IGC, peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. L'AC mettra en œuvre les mesures requises pour assurer au minimum la continuité de l'archivage des informations et la continuité des services de révocation.
Le C2SC s'assure auprès du MEN que les coûts permettant de respecter ces exigences minimales sont couverts. Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, l'AC les en avisera aussitôt que nécessaire et, au moins, sous le délai de 6 mois. De même, l'AC informera les autorités publiques concernées.

En cas d'arrêt de service, les exigences suivantes seront prises en compte :

1. La clé privée d'émission des certificats ne sera transmise en aucun cas ;
2. Toutes mesures nécessaires seront prises pour la détruire ou la rendre inopérante ;
3. Tous les certificats émis encore en cours de validité seront révoqués et les parties prenantes seront prévenues
4. Le certificat d'AC sera révoqué ;
5. L'AC communiquera au point de contact identifié sur http://ssi.gouv.fr, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement ;
6. L'AC tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus

6. MESURES DE SECURITE TECHNIQUES

6.1. GENERATION ET INSTALLATION DE BI CLES

6.1.1. Génération de bi clé

6.1.1.1. Clés de l'AC PNCN

Les clés de l'AC PNCN sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC PNCN, des porteurs de secrets et du maître de cérémonie.
Cette cérémonie de clé se fait dans un environnement totalement hors-ligne. La clé privée de l'AC PNCN est générée dans un HSM dédié.

6.1.1.2. Clés des AC Filles

Les clés des AC Filles sont générées lors de la cérémonie des clés, en présence du demandeur, de l'administrateur de l'AC PNCN et de l'AC fille, du quorum des porteurs de secrets et du maître de cérémonie.
Les clés privées des AC filles sont générées dans un environnement en ligne et la signature du certificat de l'AC fille est réalisée hors ligne par l'AC PNCN. Les clés privées des AC Filles sont générées dans un HSM partagé mais dans une partition dédiée.

6.1.2. Transmission de la clé privée à son propriétaire

Sans objet

6.1.3. Transmission de clé publique à l'AC

La demande de certificat technique est transmise à l'AC durant la cérémonie des clés sur un support USB dédié à cet usage.

6.1.4. Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et en garantit l'authentification d'origine.

6.1.5. Tailles des clés

4096 bits pour la taille des clés AC

6.1.6. Vérification de la génération des paramètres des bi clés et de leur qualité

Voir paragraphe 7.

6.1.7. Objectifs d'usages de la clé

L'utilisation de la clé privée pour l'AC PNCN et du certificat associé est limitée à la signature de certificats d'AC Filles et de LAR.
La clé privée de l'AC PNCN n'est utilisée que dans un environnement sécurisé, hors-ligne et actif que pendant la cérémonie des clés.

6.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1. Standards et mesures de sécurité pour les modules cryptographiques

Le module cryptographique de l'AC pour la génération et la mise en œuvre des clés de signature répond aux exigences énoncées par la réglementation.
Le module cryptographique de signature de certificat ne fait pas l'objet de manipulation non autorisée lors de son transport.
Le module cryptographique de signature de certificat et des informations de révocation ne fait pas l'objet de manipulation non autorisée lors de son stockage.
Le module cryptographique de signature de certificat et des informations de révocation fonctionne dans les conditions prévues par le fournisseur.
Le module cryptographique de signature de l'AC est évalué EAL 4+ et est qualifiée par l'ANSSI.

6.2.2. Contrôle des clés privées par plusieurs personnes

Il y a un contrôle de la clé privée de l'AC par au moins trois personnes.

6.2.3. Séquestre de la clé privée

Les clés privées de l'AC ne font pas l'objet de séquestre.

6.2.4. Copie de secours de la clé privée

Les clés privées de l'AC font l'objet de copie de secours dans un environnement du même niveau de sécurité que le site nominal.

6.2.5. Archivage de la clé privée

Les clés privées des AC font l'objet d'un archivage chiffré dans un coffre sécurisé.

6.2.6. Transfert de la clé privée vers / depuis le module cryptographique

Il n'y a pas de transfert de clé privée en dehors de celui réalisé vers le HSM de secours : ce transfert nécessite la présence d'au moins deux personnes, et est effectué de manière à ce que ne subsiste aucune information sensible sur le serveur.

6.2.7. Stockage de la clé privée dans le module cryptographique

Le stockage de la clé privée de l'AC est réalisé par le module cryptographique dans les conditions de sécurité définies par le profil de protection support à l'évaluation EAL 4+.

6.2.8. Méthode d'activation de la clé privée

L'activation de la clé privée de l'AC ne peut être effectuée que par la personne autorisée, et nécessite la présence de trois personnes au moins.

6.2.9. Méthode de désactivation de la clé privée

La clé privée est désactivée à partir du module cryptographique.

6.2.10. Méthode de destruction des clés privées

La destruction de la clé privée est effectuée à partir du module cryptographique.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Les modules cryptographiques de l'AC ont fait l'objet d'une qualification renforcée par l'ANSSI

6.3. AUTRES ASPECTS DE LA GESTION DES BI CLES

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC sont archivées dans le cadre de la politique d'archivage des certificats.

6.3.2. Durée de vie des bi-clés et des certificats

Les clés de signature et les certificats de l'AC ont une durée de vie de 20 ans

6.4. DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

L'initialisation et l'utilisation des données d'activation des clés d'AC se font dans le cadre d'une cérémonie des clés qui fait l'objet d'une attestation formelle à travers procès-verbal de cérémonie des clés. Ce procès-verbal est conservé par l'AC.

6.4.2. Protection des données d'activation

Les données d'activation sont remises directement au porteur de secrets qui en assure l'intégrité et la confidentialité.

6.4.3. Autres aspects liés aux données d'activation

Sans objet.

6.5. MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1. Exigences de sécurité technique spécifiques aux systèmes informatiques

6.5.1.1. Identification et authentification

Les systèmes, applications et bases de données identifient et authentifient de façon unique les utilisateurs. Toute interaction entre le système et un utilisateur n'est possible qu'après une identification et une authentification réussies. Pour chaque interaction, le système peut établir l'identité de la source de l'événement.
Les informations d'authentification sont stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés.
L'accès aux interfaces de gestion des certificats nécessitent une authentification forte basée sur au moins deux facteurs.

6.5.1.2. Contrôle d'accès

Les profils et droits d'accès aux équipements de l'OSC sont définis et documentés, ainsi que les procédures d'enregistrement et de désenregistrement des utilisateurs.
Dans tous les cas une personne non habilitée ne peut accéder aux composants de la PNCN sans l'accompagnement d'une personne habilitée.
Les systèmes applications et bases de données peuvent distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il est possible de :

- Refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet ;
- Limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet ;
- Accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel.

Quelqu'un qui n'est pas un utilisateur autorisé ne peut pas accorder ou retirer des droits d'accès à un objet. De même, seuls des utilisateurs autorisés peuvent introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.
Les supports utilisés par les intervenants autorisés de l'OSC sont manipulés conformément aux exigences du plan de classification.

6.5.1.3. Administration et exploitation

L'utilisation de programmes utilitaires est restreinte et contrôlée.
Les procédures opérationnelles d'administration et exploitation de l'IGC sont documentées, suivies et régulièrement mises à jour.
Les conditions de mise en service (paramétrage initial de sécurité des serveurs) sont documentées. Les configurations mises en œuvre permettent de renforcer le niveau de sécurité des systèmes en appliquant des mesures de durcissement.
Les conditions de fin de vie (destruction et mise au rebus) des équipements sont documentés afin de garantir la non-divulgation des informations sensibles qu'ils peuvent détenir.

L'ensemble des matériels sensibles de l'IGC fait l'objet de procédure de maintenance afin de garantir la disponibilité des fonctions et des informations. Les procédures sont documentées.
Les personnels concernés par ces procédures sont désignés formellement.
Des mesures de contrôles des actions de maintenance sont mises en application.

6.5.1.4. Intégrité des composantes

Des mesures de maîtrise de détection et de prévention sont mises en œuvre sur l'ensemble des composants de la PNCN afin de fournir une protection contre les logiciels malveillants.
Les composantes réseau de la PNCN sont maintenues dans un environnement physiquement sécurisé ; des vérifications périodiques de conformité de leur configuration sont effectuées.
Des tests réguliers de pénétration et de détection de vulnérabilités sont réalisés sur l'ensemble des composantes techniques de l'OSC.

6.5.1.5. Sécurité des flux

Des mesures de sécurité sont mises en œuvre de manière à garantir l'authentification d'origine, l'intégrité et la confidentialité le cas échéant des données échangées entre composantes intervenant dans la PNCN.

6.5.1.6. Journalisation et audit

Un suivi d'activité est possible au travers des journaux d'événements. Tous les événements liés à la sécurité des systèmes sont journalisés.
Les systèmes sont synchronisés sur l'heure UTC à la seconde près.

6.5.1.7. Supervision et contrôle

Une surveillance permanente est mise en place et des systèmes d'alarme installés pour détecter enregistrer et réagir rapidement face à toute tentative non autorisée et ou irrégulière d'accès aux ressources (physique et / ou logique).

6.5.1.8. Sensibilisation

Des procédures appropriées de sensibilisation des utilisateurs de la PNCN sont mises en œuvre.
Lorsqu'une faille de sécurité est observée sur une des composantes de l'OSC, les personnes concernées sont mises au courant de l'impact de cette faille, et un plan d'action est défini pour couvrir cette faille sous un délai raisonnable.

6.5.2. Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6. MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

Les infrastructures de développement et d'essai sont séparées des infrastructures opérationnelles de l'IGC.
Les critères de recette et validation de nouveaux systèmes d'information, de mises à niveau et nouvelles versions sont établis et des essais adéquats du système sont effectués avant sa recette et sa mise en production.
Un plan de capacité est établi pour garantir le bon traitement des certificats émis par l'AC.

6.6.1. Mesures liées à la gestion de la sécurité

L'IGC est suivie par le C2SC. L'OSC gère la remontée d'information vers l'AC qui est averti de toute modification significative.
Les évolutions des composantes font l'objet d'une remise à jour des procédures opérationnelles.

6.6.2. Niveau d'évaluation sécurité du cycle de vie des systèmes

Sans objet.

6.7. MESURES DE SECURITE RESEAU

Les équipements de filtrage en amont des composantes de la PNCN interdisent tous les flux par défaut.
Une matrice des flux est établie par l'OSC et une revue est organisée sur demande du C2SC.
Des scans périodiques de détection de vulnérabilités sur les équipements de la PNCN accessibles depuis Internet sont conduits.
Des passerelles de sécurité sont mises en place afin de protéger les composantes de la PNCN des accès non autorisés depuis l'Intranet et Internet.
La redondance des accès sur les services de l'IGC exposés sur Internet est assurée.

6.8. HORODATAGE / SYSTEME DE DATATION

Cf. 5.5.5.

7. PROFILS DES CERTIFICATS, OCSP ET DES CRL

7.1. PROFIL DU CERTIFICAT DE L'AC PNCN

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par le logiciel de cérémonie des clés
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN
NotBefore	YYMMDDHHMMSS (date de la cérémonie des clés)
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 20 ans)
Subject	Attribut Value — DirectoryString C = FR — PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE — UTF8String OU = 0002 110043015 — UTF8String OI = SI:FR-110043015 — UTF8String CN = AC PNCN — UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)

Extensions	Criticality	Valeur
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel de cérémonie des clés
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel de cérémonie des clés
Key Usage	True	
keyCertSign		Set
cRLSign		Set
Certificate Policies	False	
policyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifier-cps		
Basic Constraint	True	
cA		True
pathLenConstraint		

7.2. PROFILS DES CERTIFICATS D'AC

7.2.1. AC Fille AC AUTHENTIFICATION

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par le logiciel de cérémonie des clés
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN
NotBefore	YYMMDDHHMMSS (date de la cérémonie des clés)
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 20 ans)
Subject	Attribut Value DirectoryString C = FR PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE UTF8String OU = 0002 110043015 UTF8String OI = SI:FR-110043015 UTF8String CN = AC AUTHENTIFICATION UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)

Extensions	Criticality	Valeur
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel de cérémonie des clés
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel de cérémonie des clés
Key Usage	True	
keyCertSign		Set
cRLSign		Set
Certificate Policies	False	
policyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifier-cps		
Basic Constraint	True	
cA		True
pathLenConstraint		0
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_PNCN.crl
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_PNCN.p7b

7.2.2. AC Fille AC SIGNATURE

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par le logiciel de cérémonie des clés
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN
NotBefore	YYMMDDHHMMSS (date de la cérémonie des clés)
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 20 ans)
Subject	Attribut Value DirectoryString C = FR PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE UTF8String OU = 0002 110043015 UTF8String OI = SI:FR-110043015 UTF8String CN = AC SIGNATURE UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)

Extensions	Criticality	Valeur
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel de cérémonie des clés
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel de cérémonie des clés
Key Usage	True	
keyCertSign		Set
cRLSign		Set
Certificate Policies	False	
policyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifier-cps		
Basic Constraint	True	
cA		True
pathLenConstraint		0
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_PNCN.crl
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_PNCN.p7b

7.2.3. AC Fille AC SERVICES

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par le logiciel de cérémonie des clés
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN
NotBefore	YYMMDDHHMMSS (date de la cérémonie des clés)
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 20 ans)
Subject	Attribut Value DirectoryString C = FR PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE UTF8String OU = 0002 110043015 UTF8String OI = SI:FR-110043015 UTF8String CN = AC SERVICES UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)

Extensions	Criticality	Valeur
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel de cérémonie des clés
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel de cérémonie des clés
Key Usage	True	
keyCertSign		Set
cRLSign		Set
Certificate Policies	False	
policyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifier-cps		
Basic Constraint	True	
cA		True
pathLenConstraint		0
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_PNCN.crl
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_PNCN.p7b

7.2.4. AC Fille AC HORODATAGE

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par le logiciel de cérémonie des clés
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN
NotBefore	YYMMDDHHMMSS (date de la cérémonie des clés)
NotAfter	YYMMDDHHMMSS (date de la cérémonie des clés + 20 ans)
Subject	Attribut Value — DirectoryString C = FR — PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE — UTF8String OU = 0002 110043015 — UTF8String OI = SI:FR-110043015 — UTF8String CN = AC HORODATAGE — UTF8String
Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)
Key size	4096
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.13)

DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality	Valeur
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel de cérémonie des clés
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel de cérémonie des clés
Key Usage	True	
keyCertSign		Set
cRLSign		Set
Certificate Policies	False	
policyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifier-cps		
Basic Constraint	True	
cA		True
pathLenConstraint		0
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_PNCN.crl
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_PNCN.p7b

7.3. PROFILS DES ARLS

Un ensemble de 12 ARLs est généré en Cérémonie de Clés et ces ARLs sont signées par l'AC.
Chaque ARL doit avoir :

- Une durée de 45 jours
- Une période de renouvellement de 15 jours.

Il n'y a pas de delta CRL.

Field	Value		
Version	1 (Version=2)		
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC PNCN		
ThisUpdate	YYMMDDHHMMSS (date d'émission de l'ARL)		
NextUpdate	YYMMDDHHMMSS (date d'émission de l'ARL + 45 jours)		
Signature (algorithm & OID)	Sha512WithRSAEncryption (1.2.840.113549.1.1.11)		
Revoked Certificate	userCertificate : Serial Number du certificat d'AC révoqué revocationDate : date de révocation du certificat au format UTCTime crlEntryExtensions : aucune extension d'entrée n'est utilisée		
CRL Extension	**Include**	**Critical (True/False)**	**Value**
CRLNumber	Yes	False	Integer incremented, start = 1
AKI	Yes	False	Issuer key hash

8. AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

8.1. FREQUENCES ET / OU CIRCONSTANCES DES 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. Cet audit interne peut être mené par des équipes internes au MEN ou bien à travers des prestations externes. Le suivi et le pilotage de l'audit interne reste sous le contrôle d'un rôle de confiance de l'AC identifié comme « auditeur interne ».

8.2. IDENTITES : QUALIFICATION DES EVALUATEURS

Le contrôleur est compétent pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non-conformités qui pourraient compromettre la sécurité du service offert.

8.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

Le contrôleur est désigné par l'AC. Il est indépendant de l'AC et de l'OSC.

8.4. PERIMETRE DES EVALUATIONS

Le contrôleur procède de manière régulière à des contrôles de conformité de la mise en œuvre :

- Des politiques de certification
- Des déclarations de pratique de certification
- Des services mis en œuvre

Il a notamment pour objectif de s'assurer que les pratiques mises en œuvre permettent de répondre aux exigences attendues par les niveaux de qualification obtenus par la PNCN. Il s'assure également que les processus de gestion du cycle de vie des certificats sont conformes aux procédures rédigées.

8.5. ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC un avis qui peut être « réussite, échec, ou à confirmer ».
En cas d'échec, l'équipe d'audit remet des recommandations à l'AC ; le choix des mesures à appliquer appartient à l'AC.
En cas de résultat « à confirmer », l'équipe d'audit identifie les non-conformités, et les hiérarchisent ; il appartient au C2SC de proposer un calendrier de résolution des non-conformités ; un contrôle de vérification permettra de lever les non-conformités identifiées.
En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC.

8.6. COMMUNICATION DES RESULTATS

Dans le cas d'une qualification de l'AC, les résultats d'audits sont tenus à la disposition de l'organisme en charge de la qualification.

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1. 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 LAR n'est jamais facturée.

9.2. RESPONSABILITE FINANCIERE

9.2.1. Couverture par les assurances

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

9.2.2. 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.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Pas d'exigence spécifique.

9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1. Périmètre des informations confidentielles

L'AC et l'OSC mettent en place un inventaire de tous les biens informationnels et procèdent à une classification de manière à définir des exigences de protection en accord avec les besoins.
En particulier, les informations suivantes sont traitées comme confidentielles :

- Les clés privées d'AC
- Les scripts de cérémonies
- Les codes d'activation des parts de secrets
- Les journaux d'événements
- La DPC et les procédures internes de l'AC
- Les dossiers de demande de certificats d'AC
- Les causes de révocation des certificats

9.3.2. Informations hors du périmètre des informations confidentielles

Sans objet

9.3.3. Responsabilités en termes de protection des informations confidentielles

L'AC s'engage à traiter (et à faire traiter par les différentes parties prenantes) les informations confidentielles recueillies dans le respect des lois et règlements en vigueur.

9.4. PROTECTION DES DONNEES PERSONNELLES

9.4.1. Politique de protection des données 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.

9.4.2. Informations à caractère personnel

Les informations à caractère personnel sont les suivantes :

- Les causes de révocation qui restent confidentielles et ne sont pas publiées ;
- Les informations d'enregistrement ;
- Le contenu des certificats.

9.4.3. Informations à caractère non personnel

Pas d'exigence spécifique.

9.4.4. Responsabilité en termes de protection des données 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 lui incombent au titre de la présente PC et des traitements de données à caractère personnel qui seraient réalisés.

9.4.5. Notification et consentement d'utilisation des données personnelles

Conformément aux législations et réglementations en vigueur, en particulier sur le territoire français, les informations personnelles remises à l'AC ne sont ni divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du responsable de l'AC, décision judiciaire ou autre autorisation légale.

9.4.6. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

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

9.4.7. Autres circonstances de divulgation d'informations personnelles

Pas d'exigence spécifique.

9.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

La fourniture de service par l'AC ne saurait être interprétée comme entraînant la cession d'un quelconque droit de propriété intellectuelle.

9.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES

9.6.1. Autorités de certification

Au titre des présentes PC, et pour le domaine qu'elles couvrent (voir paragraphe 1.4), l'AC garantit le respect des engagements décrits dans le présent document.
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
- 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.

9.6.2. Autorité d'enregistrement

Voir paragraphes 1.3.3.

9.6.3. 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 des certificats de la chaîne d'AC et contrôler la validité des certificats

9.6.4. Autres participants

Voir paragraphes 1.3.2.

9.7. 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.

9.8. 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, des LAR ainsi que de tout autre équipement ou logiciel mis à disposition.

9.9. INDEMNITES

Sans objet.

9.10. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1. Durée de validité

Le présent document est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2. Fin anticipée de validité

Sauf événement exceptionnel lié à la sécurité, les évolutions du présent document n'imposent pas la révocation des certificats déjà émis.

9.10.3. Effets de la fin de validité et clauses restant applicables

La fin de validité des présentes PC rend caduques les engagements de l'AC qui y sont portés, à l'exception des clauses traitant de la fin de vie des servies de l'AC, de l'archivage et du transfert d'activité.

9.11. NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

En cas de changement de toute nature intervenant dans la composition des services de l'AC, l'AC s'engage à :

- Au plus tard 6 mois avant le début de l'opération, faire valider par le C2SC ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'IGC et de ses différentes composantes.
- Au plus tard 1 mois après la fin de l'opération, en informer, le cas échéant, l'organisme de qualification

9.12. AMENDEMENTS A LA PC

9.12.1. Procédures d'amendements

L'AC s'engage à contrôler que tout changement apporté au présent document reste conforme aux objectifs de conformité aux exigences réglementaires en matière de qualification de PSCo.

9.12.2. Mécanisme et période d'information sur les amendements

Toute nouvelle version est disponible en format électronique sur le site Internet identifié au paragraphe 2.1 et dans un délai maximum de 24 heures suite à son approbation par le C2SC. Elle prend effet dès sa publication.

9.12.3. Circonstances selon lesquelles l'OID doit être changé

Toute évolution majeure de la PC ayant un impact majeur sur les certificats déjà émis sera signifiée par une évolution de l'OID.

9.12.4. Informations aux utilisateurs

Toute nouvelle version de la présente Politique de Certification fera l'objet d'une information sur le site Internet identifié au paragraphe 2.1 à destination des porteurs et des applications utilisatrices.

Cette information sera préalable à toute émission d'un certificat final conforme aux nouvelles exigences de la nouvelle Politique de Certification.

9.13. DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

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

9.14. JURIDICTIONS COMPETENTES

La présente Politique de Certification est soumise au droit français.
Tout litige relatif à la validité, l'interprétation, et/ou l'exécution de la présente Politique de Certification sera soumis aux tribunaux compétents de la cour d'appel de Paris.

9.15. CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

En sus de la règlementation RGPD, l'AC PNCN vise une certification aux normes ETSI 319401, ETSI 319411-1.

9.16. DISPOSITIONS DIVERSES

9.16.1. Accord global

Pas d'exigence spécifique

9.16.2. Transfert d'activités

Cf. chapitre 5.8

9.16.3. Conséquences d'une clause non valide

Pas d'exigence spécifique

9.16.4. Application et renonciation

Pas d'exigence spécifique

9.16.5. 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.

9.17. AUTRES DISPOSITIONS

Les politiques et procédures de l'AC sont non-discriminatoires.

9.18. CONDITIONS GENERALES D'UTILISATION

Sans objet.

10. DOCUMENTS ASSOCIES

10.1. DOCUMENTS APPLICABLES

[A1]	RFC 3647. Internet X509 PKI certificate policy and certificate practice statement framework
[A2]	Règlement Européen eIDAS 910/2014
[A3]	ISO/IEC 9594. Distinguished name
[A4]	Règlement (UE) 2016/679 du Parlement européen et du Conseil 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
[A5]	EN 319401 « General Policy Requirements for Trust Service Providers »
[A6]	EN 319411-1 « General requirements »
[A8]	EN 319412-1 « Overview and common data structures »
[A9]	EN 319412-2 « Certificate profile for certificates issued to natural persons »

10.2. DOCUMENTS DE REFERENCE

S/O

11. ANNEXE 1 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

11.1. EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le module cryptographique utilisé pour la génération des certificats et des LCR répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et leur destruction sûre en fin de vie
- Etre capable d'identifier et d'authentifier ses utilisateurs
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur
- Permettre de créer une signature électronique sécurisée pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité
- Si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration
- Détecter les tentatives d'altération physique et entrer dans un état sûr quand une tentative d'altération est détectée

11.2. EXIGENCES SUR LA CERTIFICATION

Le module est certifié conformément aux exigences ci-dessus, et a fait l'objet d'une qualification (EAL4+ avec une résistance élevée des mécanismes).