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

Plateforme Nationale de Confiance Numérique

Politique de Certification
Pour les certificats d'authentification et de chiffrement de personnes physiques

PC AC Authentification – Format RFC 3647

Statut du document : validé
Version : 2.1

PUBLIE

Entrée en vigueur le 09/07/2024

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 et en particulier des exigences définies dans les documents [A5], [A6], [A7], [A8] mise à part la mise en œuvre d'un service OCSP. Cette Politique de Certification couvre les niveaux suivants comme établi dans [A6] :

- LCP
- NCP
- NCP+

Le MEN s'est positionné comme prestataire de service de certification électronique, en proposant des services permettant 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 AUTHENTIFICATION.
Sa structure est conforme au RFC 3647, [A1].

1.2. IDENTIFICATION DU DOCUMENT

Le numéro d'OID du présent document est 1.2.250.1.535.2.2.2.3.1.1.3
Les profils de certificats suivants sont émis à travers la présente Politique de Certification :

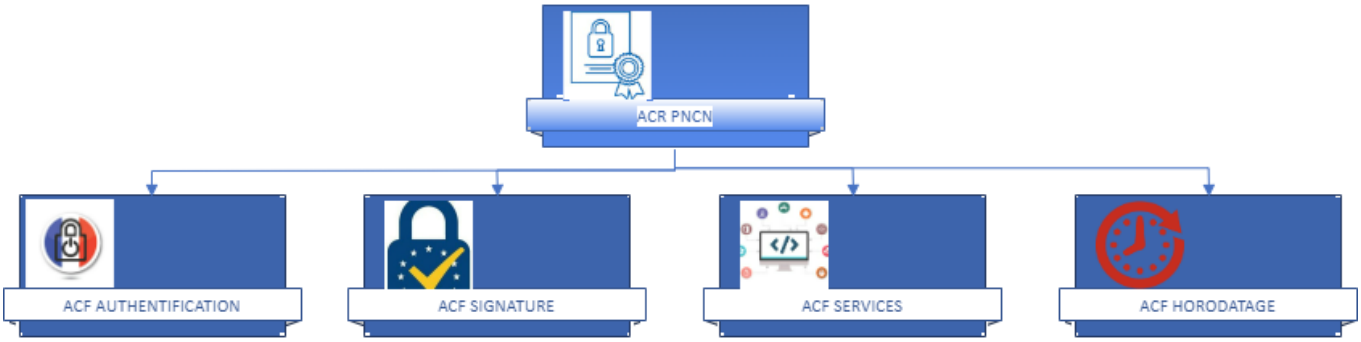
1.2.250.1.535.2.2.2.3.6.1.1	Personnes_Authentification
1.2.250.1.535.2.2.2.3.6.2.1	Personnes_Authentification_Decrochage
1.2.250.1.535.2.2.2.3.6.3.1	Personnes_Chiffrement
1.2.250.1.535.2.2.2.3.6.8.1	Personnes_Chiffrement_Matériel
1.2.250.1.535.2.2.2.3.6.4.1	Personne_Authentification_Matériel
1.2.250.1.535.2.2.2.3.6.6.1	Personnes_Authentification_VSC
1.2.250.1.535.2.2.2.3.6.7.1	OCSP_Authentification

1.3. ENTITES INTERVENANT DANS L'IGC

Le certificat de l'AC AUTHENTIFICATION 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 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 utilisés en support de la fonction d'authentification et de chiffrement.
Ce sont :

- Les bi-clés et certificats générés sur des supports cryptographiques matériels permettant de s'authentifier sur des applicatifs métiers du MEN ou des partenaires,
- Les bi-clés et certificats générés sous format logiciel permettant de chiffrer des documents ou des messages,
- Les bi-clés et certificats générés sous format logiciel permettant de s'authentifier.

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 1.2.

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 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

1.3.3. Autorité 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.

1.3.4. Officier de Confiance Numérique (OCN)

Il s'agit des opérateurs de saisie et de validation des demandes de certificats. Il y a des OCN au niveau de l'AE centralisée (OCN centraux) et des OCN au niveau de chaque Académie ou Département.
Suivant les gammes de certificats concernées, la validation peut se faire qu'au niveau de l'AE centrale.

1.3.5. Porteurs de certificats

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

1.3.6. Responsable hiérarchique

Il s'agit du responsable d'un agent au sein de l'entité à laquelle il appartient. Il est en charge d'assurer avec les OCN la validation des demandes de certificat, notamment valider la légitimité d'un demandeur de certificat à faire une demande de certificat.
Dans le cas des partenaires, le porteur n'est pas un agent du MEN. Le rôle de responsable hiérarchique est alors joué par un agent ayant reçu la délégation d'une personne formellement identifiée au niveau du MEN.
Dans la suite du document, la notion de « responsable hiérarchique » s'applique sans préjuger du fait que le porteur soit un agent ou un partenaire.

1.3.7. 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 d'authentification ou de chiffrement.

1.4. USAGE DES CERTIFICATS

1.4.1. Domaines d'utilisation applicables

Les certificats finaux sont utilisés soit pour s'authentifier sur des applicatifs métiers du MEN ou des partenaires, soit pour chiffrer des données dans le cadre de ses activités professionnelles et dans le respect des délégations de signature établies.

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 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). Le comité se réunit mensuellement pour traiter des points liés à la PNCN. Le bureau DNE - Socle 4 est le responsable de la sécurité.

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 : pncn@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

Abréviation	Signification
AC	**A**utorité de **C**ertification
ACF	**A**utorité de **C**ertification **F**ille
ACR	**A**utorité de **C**ertification **R**acine
AE	**A**utorité d'**E**nregistrement
AED	**A**utorité d'**E**nregistrement **D**éléguée
ANSSI	**A**gence **N**ationale de **S**écurité des **S**ystèmes d'**I**nformation
C2SC	**C**omité de **S**uivi des **S**ervices de **C**onfiance
CGU	**C**onditions **G**énérales d'**U**tilisation
COSSIM	**C**entre **O**pérationnel de **S**écurité des **S**ystèmes d'**I**nformation Ministériel
DN	**D**istinguished **N**ame
DNE	**D**épartement **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)
HSM	**H**ardware **S**ecurity **M**odule
IGC	**I**nfrastructure de **G**estion de **C**lés
LAR	**L**iste des **A**utorités **R**évoquées
LCP	**L**ightweight **C**ertificate **P**olicy
LCR	**L**iste des **C**ertificats **R**évoqués
MEN	**M**inistère de l'**E**ducation **N**ationale
MENJS	**M**inistère de l'**E**ducation **N**ationale de la **J**eunesse et des **S**ports
NCP	**N**ormalized **C**ertificate **P**olicy
NCP +	**N**ormalized **C**ertificate **P**olicy Plus
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
PIN	**P**ersonal **I**dentification **N**umber
PKI	**P**ublic **K**ey **I**nfrastructure
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
RGPD	**R**èglement **G**énéral pour la **P**rotection des **D**onnées
SIEM	**S**ecurity **I**nformation **E**vent **M**anagement
SIREN	**S**ystème d'**I**dentification du **R**épertoire des **EN**treprises
SIRET	**S**ystème d'**I**dentification du **R**épertoire des **ET**ablissements

Abréviation	Signification
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
VSC	**V**isual **S**tudio **C**ode

1.6.2. Définitions

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'un 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 ainsi que la Politique de Certification de l'AC Racine « AC PNCN » [R2]
- 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 AUTHENTIFICATION en cours de validité, ainsi que les certificats en cours de validité de l'AC PNCN (hiérarchie à laquelle est rattachée l'AC AUTHENTIFICATION)
- 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.

2.3. DELAIS ET FREQUENCES DE PUBLICATION

Les politiques de certification 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.

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 – PC, CGU, formulaires) ou bien de manière automatique par des scripts programmés au niveau du serveur de publication (publication des nouvelles LCR).
Le processus de publication de la LCR permet de s'assurer de :

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

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 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 :

- Pour les certificats de personnes :
    - 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 »
    - 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'

- Pour les certificats OCSP :
    - 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 »
    - Le nom du certificat OCSP avec un numéro de version dans le champ « commonName »

Ces champs sont identiques qu'il s'agisse de la production d'un certificat logiciel ou d'un certificat matériel.

3.1.3. Anonymisation ou pseudonymisation des porteurs

Sans objet

3.1.4. Règles d'interprétation des différentes formes de noms

3.1.4.1. Pour les certificats logiciels

Les informations portées dans les certificats sont issues de déclarations des demandeurs. Cela peut se faire de manière déclarative seule ou bien contenue dans un fichier listant une série de porteurs à créer. A minima la demande contient le nom et prénoms des futurs porteurs de certificats. Les autres informations nécessaires à la production des certificats sont saisies par l'OCN sous sa responsabilité.

3.1.4.2. Pour les certificats matériels

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

3.1.5. Unicité des noms

Le champ « serialNumber » des certificats permet de garantir l'unicité de l'identité du porteur dans le contenu du certificat. 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'.

Un même DN peut être présent dans plusieurs certificats en même temps, chacun des certificats correspondants étant délivrés au même porteur.

3.1.6. Identification, authentification et rôle des marques déposées

Pour les marques, dénominations sociales ou autres signes distinctifs, l'AE 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

3.2.1.1. 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).

3.2.1.2. Pour les certificats matériels

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 excepté pour les certificats de chiffrement qui font l'objet d'un séquestre préalable par l'Autorité de Certification et d'une installation dans le support cryptographique.
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.

3.2.2. Validation de l'identité d'un organisme

3.2.2.1. Pour les certificats logiciels

L'organisation du futur porteur est déterminée par l'OCN qui se charge de saisir les informations nécessaires. Ces éléments peuvent être validés le cas échéant avec le responsable hiérarchique du ou des porteurs par l'OCN.

3.2.2.2. Pour les certificats matériels

Les certificats produits sont destinés à des personnes physiques rattachées 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.

3.2.3. Validation de l'identité d'un individu

3.2.3.1. Enregistrement d'un porteur pour un certificat logiciel

L'OCN est en charge de s'assurer de l'identité du futur porteur auprès d'un responsable hiérarchique du porteur. Il se base ensuite sur les éléments déclarés dans la demande.

3.2.3.2. Enregistrement d'un porteur pour un certificat sur support matériel

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.

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.

3.2.3.3. 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.

3.2.3.4. 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.

3.2.4. Informations non vérifiées du porteur

Sans objet

3.2.5. Validation de l'autorité du demandeur

3.2.5.1. Pour les certificats logiciels

L'autorité du demandeur de certificat est vérifiée par l'OCN en se rapprochant d'un responsable hiérarchique du ou des porteurs pour lesquels des certificats sont demandés.

3.2.5.2. Pour les certificats matériels

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.

3.2.6. 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 et de ses partenaires. 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 AUTHENTIFICATION 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 AUTHENTIFICATION pourra attendre des AC demandant un accord de certification de respecter les formats des certificats suivant la norme [A7], [A8].

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 porteur devra procéder comme pour une demande initiale (cf. paragraphe 3.2).

3.4. IDENTIFICATION ET VALIDATION D'UNE DEMANDE 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 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. Elle peut être effectuée par Internet (voir **1.5.2**).Le porteur se connecte directement sur les interfaces de révocation mises à disposition par l'AC.
L'identification du porteur 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.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. DEMANDE DE CERTIFICAT

4.1.1. Origine d'une demande de certificat

4.1.1.1. 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

4.1.1.2. Pour les certificats matériels

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

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

4.1.2.1. 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.

4.1.2.2. Pour les certificats matériels

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
- La validation par le responsable hiérarchique de la demande de certificat
- 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 signé par le porteur

4.2. TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

4.2.1.1. 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

4.2.1.2. Pour les certificats matériels

L'identité du porteur, 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.

4.2.2. 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 par courriel ; elle peut être également formulée par l'OCN lors du face-à-face.
Pour les certificats matériels, si la demande est validée, l'OCN remet au porteur un support cryptographique.

4.2.3. 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.

4.3. DELIVRANCE DU CERTIFICAT

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

4.3.1.1. Pour les certificats logiciels :

Après avoir validé la demande, l'OCN fait produire par la PKI un containeur sécurisé au format PKCS#12 contenant :

- La clé privée
- Le certificat final

L'OCN réalise ensuite les opérations suivantes :

- Transmission du fichier PKCS#12 au responsable hiérarchique du porteur par email
- Transmission du mot de passe de protection du fichier PKCS#12 au porteur par email

4.3.1.2. Pour les certificats matériels :

L'OCN dispose des outils permettant de faire le retrait du certificat avec le support cryptographique remis au porteur. Il réalise les étapes en sa présence et lui fait saisir le code PIN de son support cryptographique.
Alternativement le porteur peut initier seul le retrait de certificat sur son support cryptographique à l'aide d'un code d'activation qui lui aura été communiqué en amont de la remise du support en main propre.
La remise et l'activation du support cryptographique sont formalisées dans une charte de remise et d'utilisation du support cryptographique signée par le porteur et contresignée par l'OCN. Cette charte est datée.
Les supports cryptographiques 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.

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

Le processus est réalisé en présence du porteur.

4.4. ACCEPTATION DU CERTIFICAT

4.4.1. Démarche d'acceptation du certificat

4.4.1.1. Pour les certificats logiciels :

Le mail transmis au porteur contient un lien permettant au porteur de consulter les Conditions Générales d'Utilisation du certificat. L'acceptation de son certificat est implicite.

4.4.1.2. Pour les certificats matériels :

Le certificat est élaboré en ligne, et transmis lors de la phase d'initialisation du support cryptographique.
Le porteur accepte explicitement son certificat en signant la charte de remise et d'utilisation du support cryptographique.
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, l'OCN procède alors à la révocation immédiate du certificat concerné.

4.4.2. Publication du certificat

Les certificats finaux ne sont pas publiés.

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 par le porteur

4.5.1.1. Certificat d'authentification

L'utilisation de la clé privée par le porteur est limitée à l'authentification dans le cadre de ces activités professionnelles pour le MEN. Cet usage est indiqué explicitement dans les extensions du certificat qui présente les keyUsage « digitalSignature ».

4.5.1.2. Certificat de chiffrement

L'utilisation de la clé privée par le porteur est limitée au chiffrement de données. Cet usage est indiqué explicitement dans les extensions du certificat qui présente les keyUsage « keyEncipherment » et « dataEncipherment ».

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

L'utilisation du certificat est limitée à la vérification de l'identité d'une personne reconnue par le MEN ou le chiffrement de données.

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 au porteur 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 au porteur 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 au porteur 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
- Création d'un nouveau certificat (avec nouvelles bi-clés) par le porteur avant l'expiration de son certificat précédent
- Décision du porteur
- Erreur dans le dossier de demande de certificat
- Refus du certificat par le porteur durant la phase de remise
- Destruction, altération du support cryptographique ou de ses fonctions
- Départ du porteur de certificat
- 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 AUTHENTIFICATION
- Cessation d'activité de l'AC PNCN

4.9.1.2. Certificats d'AC

Voir PC de l'AC PNCN [R2]

4.9.2. Origine d'une demande de révocation

Les personnes pouvant demander une révocation sont les suivantes :

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

4.9.3. Procédure de traitement d'une demande de révocation

4.9.3.1. Certificat final

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. 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.

4.9.3.2. Certificats d'AC

Voir PC de l'AC PNCN [R2]

4.9.4. Délai accordé au porteur pour formuler la demande de révocation

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

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

4.9.5.1. Certificats de porteur

Le délai maximum de traitement est de 24 heures.

4.9.5.2. Certificats d'AC

Voir PC de l'AC PNCN [R2]

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 :

- Recourir au service OCSP,

Ou

- 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

4.9.7. Fréquence d'établissement des LCR

Les LCR sont émises à minima toutes les 24h.

4.9.8. Délai maximum de publication d'une LCR

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

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 LCR sont au format v2, publiées sur le site internet identifié au paragraphe2.1.

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

Les certificats de chiffrement font l'objet d'un séquestre. La clé privée est générée en central et est conservée de manière sécurisée par l'AC.

4.12.1. Politique et pratiques de recouvrement par séquestre de clés

Les clés de chiffrement sont conservées dans une base de données de séquestre. Un rôle de confiance en charge du dé séquestre est mis en œuvre. Le processus de dés équestre est donc un processus organisationnel qui met en œuvre des accès spécifiques par les personnes habilitées et dont les différentes actions sont tracées dans un procès-verbal.

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 du porteur, gestion des révocations et 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).
Les OCN mettent également en place des mesures physiques ou logiques de contrôle d'accès afin de limiter l'accès aux moyens de validation et aux dossiers archivés.

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 du MEN – socle 4 à travers la Direction du Numérique de l'Education Nationale (DNE).
La gouvernance est assurée à travers le « Bureau de la sécurité » 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'Autorité d'enregistrement :
    - Saisie et validation des demandes de certificats en central (AE centralisée) : Officiers de Confiance Numérique au sein de la PNCN
    - Validation des demandes de révocation : Officiers de Confiance Numérique au sein de la PNCN
    - Gestion du recouvrement des clés de chiffrement : personnes au sein de la PNCN disposant des habilitations sur les interfaces de la PKI permettant de faire un dé séquestre des clés privées des certificats de chiffrement.

- 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.
Le rôle d'Officier de Confiance Numérique central n'est pas cumulé avec un rôle lui permettant d'accéder au paramétrage des interfaces techniques d'AE. Il n'est que simple utilisateur de ces interfaces.
Le rôle d'Officier de Confiance Numérique académique n'a pas de rôle opérationnel sur les composantes de la PNCN.

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 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).

5.4.2. Fréquence de traitement des journaux d'événements

Les journaux d'événements sont exploités :

- De manière quotidienne dans le cadre de processus automatisé de contrôle
- Systématiquement en cas de remontée d'événement anormal
- De manière mensuelle, à travers un rapprochement entre les activités de l'AE et les traces des systèmes de l'OSC

5.4.3. Période de conservation des journaux d'événements

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.

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 procédures de sauvegarde des journaux sont quotidiennes par delta avec les sauvegardes précédentes, et globales de manière hebdomadaire.

5.4.6. Système de collecte des journaux d'événements

Les événements enregistrés au sein de l'IGC sont centralisés au sein d'un SIEM.

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

Sans objet

5.4.8. Evaluation des vulnérabilités

Le contrôle des journaux d'événement système et technique est continu et quotidien afin de permettre une anticipation des vulnérabilités, et des remontées d'alerte en cas de vulnérabilités. Ces contrôles sont réalisés via des processus automatiques qui permettent de détecter des anomalies.
Le contrôle des journaux des événements fonctionnels est réalisé à la demande en cas de litige, ou pour analyse de comportement de l'IGC.

Une revue mensuelle des événements anormaux est réalisée par le C2SC en faisant le rapprochement des dossiers traités par les AE (par les OCN) et les traces fonctionnelles obtenues par l'OSC. Ce rapprochement se fait sur la base d'un échantillonnage.

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 et CGU
- Certificats, LAR et LCR publiés
- Fiches de postes des rôles de confiance signées
- Dossiers de demande de certificats finaux
- 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 de l'AC AUTHENTIFICATION	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

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'IGC sont synchronisés sur un même serveur synchronisé avec l'heure universelle.

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 2 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 AUTHENTIFICATION est de 20 ans. La durée de vie des certificats est de 3 ans pour les certificats émis par l'AC AUTHENTIFICATION.

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 AUTHENTIFICATION ;
- 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 OCN et les porteurs correspondants seront prévenus ;
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 AUTHENTIFICATION

Voir PC AC PNCN [R2]

6.1.1.2. Clés porteurs générées par l'AC

Cela s'applique exclusivement pour les certificats de chiffrement et pour les certificats logiciels. La bi-clé est générée par l'AC après validation de la demande par l'OCN. Le processus consiste à créer un conteneur au format PKCS#12 contenant la clé privée, le certificat et la chaîne d'AC. Pour les certificats de chiffrement, ces éléments sont alors importés directement dans le support cryptographique remis au porteur.

6.1.1.3. Clés porteurs générées par le porteur

Pour les certificats de niveau NCP et NCP+, la génération des bi clés du porteur est effectuée directement dans le support cryptographique.
Le processus d'affectation au porteur du support cryptographique est déclenché par l'OCN et il s'assure que le dispositif à initialiser est un support cryptographique reconnu par l'AC, en effectuant la mise en place d'un canal sécurisé basé sur des clés sécrètes échangées entre l'OSC et le fournisseur des supports cryptographiques.
Le porteur initialise le code d'utilisation du support, code qu'il est seul à connaitre.

6.1.2. Transmission de la clé privée à son propriétaire

Pour les certificats logiciels, la clé privée est dans le conteneur PKCS#12 transmis par email à l'OCN du porteur. L'OCN est alors en charge de transmettre ce containeur au porteur concerné.
Concernant les certificats de chiffrement, la clé privée est installée sur le support cryptographique via l'import du containeur PKCS#12 sur le support.

6.1.3. Transmission de clé publique à l'AC

Le protocole utilisé pour la transmission de la clé publique du porteur à l'AC est accompagné de mesures garantissant l'intégrité et l'authentification d'origine. La procédure de délivrance du certificat est liée de manière sécurisée à l'enregistrement associé ou au changement de bi-clé, ainsi qu'à la fourniture de la clé publique par le porteur.

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
2048 bits pour la taille des clés des porteurs

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 d'AC et du certificat associé est limitée à la signature de certificats et de LCR, comme définie dans le paragraphe 7. La clé privée d'AC n'est utilisée que dans un environnement HSM qualifié.

6.1.7.1. Bi-clés et certificats d'authentification

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

6.1.7.2. Bi-clés et certificats de chiffrement

L'utilisation de la clé privée du porteur et du certificat associé est limitée au chiffrement ou au déchiffrement de données.

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

6.2.1.1. Module cryptographique de l'AC

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.

6.2.1.2. Module cryptographique des porteurs

Les supports cryptographiques mis à la disposition des porteurs sont évalués EAL 4+ et qualifiés par l'ANSSI.

6.2.2. Contrôle des clés privées par plusieurs personnes

6.2.2.1. Module cryptographique de l'AC

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

6.2.2.2. Module cryptographique des porteurs

Le support cryptographique du porteur est sous son contrôle exclusif.

6.2.3. Séquestre de la clé privée

Les clés privées des porteurs disposant d'un certificat de chiffrement font l'objet d'un séquestre (voir 4.12).

6.2.4. Copie de secours de la clé privée

6.2.4.1. Clés de l'AC

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.

6.2.4.2. Clés des porteurs

Les clés privées des porteurs ne font l'objet de copie de secours que pour les certificats de chiffrement. Les copies sont sécurisées au même niveau que la base de séquestre initiale.

6.2.5. Archivage de la clé privée

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

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

6.2.6.1. Transfert de la clé privée de l'AC

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.

6.2.6.2. Transfert de la clé privée des porteurs

Les clés privées de chiffrement des porteurs peuvent être exportées en dehors du support cryptographique. Cette opération reste sous la seule responsabilité du porteur.

6.2.7. Stockage de la clé privée dans le module cryptographique

6.2.7.1. Stockage de la clé privée de l'AC

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+.

6.2.7.2. Stockage de la clé privée des porteurs

6.2.7.2.1 Pour les certificats logiciels

Les certificats logiciels sont stockés initialement dans le containeur PKCS#12 fourni au porteur. Ce dernier est ensuite en charge et responsable du stockage de la clé privée dans son environnement. L'AC ne limite pas le type de support de stockage et autorise : le stockage dans le magasin de certificats du système d'exploitation, le stockage sur le disque dur de l'environnement du porteur dans le containeur PKCS12, stockage sur un support externe sous le contrôle du porteur, stockage dans un environnement sécurisé de l'ordinateur du porteur.

6.2.7.2.2 Pour les certificats matériels

Le stockage de la clé privée est réalisé par le support 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

6.2.8.1. Activation de la clé privée de l'AC

L'activation de la clé privée se fait au démarrage du HSM sous contrôle de l'administrateur HSM.

6.2.8.2. Activation de la clé privée des porteurs

6.2.8.2.1 Pour les certificats logiciels

L'activation de la clé privée par le porteur dépend de l'environnement et du choix du porteur. L'AC recommande que le porteur protège l'accès à sa clé privée par un mot de passe.

6.2.8.2.2 Pour les certificats matériels

La clé privée est activée à l'aide d'un code PIN personnel et connu exclusivement du porteur.

6.2.9. Méthode de désactivation de la clé privée

6.2.9.1. Désactivation de la clé privée de l'AC

La clé privée est désactivée à partir du module cryptographique.

6.2.9.2. Désactivation de la clé privée des porteurs

6.2.9.2.1 Pour les certificats logiciels

La clé privée du porteur est désactivée par effacement logique de cette dernière.

6.2.9.2.2 Pour les certificats matériels

La clé privée est désactivée à partir du support cryptographique.

6.2.10. Méthode de destruction des clés privées

6.2.10.1. Destruction de la clé privée de l'AC

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

6.2.10.2. Destruction de la clé privée des porteurs

6.2.10.2.1 Pour les certificats logiciels

La clé privée du porteur est détruite par effacement définitif de cette dernière.

6.2.10.2.2 Pour les certificats matériels

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

6.2.11. Niveau d'évaluation sécurité du module cryptographique

6.2.11.1. Module cryptographique de l'AC

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

6.2.11.2. Module cryptographique des porteurs

Les supports cryptographiques font l'objet d'une évaluation EAL 4+ et d'une qualification au niveau 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 et des porteurs 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
Les clés privées et les certificats des porteurs ont une durée de vie de 3 ans.

6.4. DONNEES D'ACTIVATION

6.4.1. Génération et installation des données d'activation

6.4.1.1. Génération et installation des données d'activation correspondant à la clé privée de l'AC

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.

6.4.1.2. Génération et installation des données d'activation correspondant à la clé privée des porteurs

6.4.1.2.1 Pour les certificats logiciels

Les données d'activation de la clé privée sont au choix du porteur au moment de l'installation de son certificat dans son environnement. La mesure de protection consiste à protéger l'accès à la clé privée par un mot de passe. Lorsque le porteur utilise directement le containeur au format PKCS#12 qui lui a été transmis, il est recommandé au porteur de changer le mot de passe de protection et de choisir un mot de passe qui lui est personnel.

6.4.1.2.2 Pour les certificats matériels

Les données d'activation sont nécessaires à l'initialisation du support cryptographique et sont choisies par le porteur lui-même. Cette phase d'activation du support cryptographique permet au porteur de générer son propre code PIN.

6.4.2. Protection des données d'activation

6.4.2.1. Pour les certificats logiciels

Les données d'activation sont au choix et sous la responsabilité du porteur.

6.4.2.2. Pour les certificats matériels

Les données d'activation sont transmises directement au porteur du support cryptographique.

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.
Au niveau des accès logiques, des droits sont positionnés sur les différentes interfaces et composants, de manière à garantir les habilitations des personnes en fonction du rôle de confiance affecté.
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.

6.5.1.9. Exigences spécifiques au support cryptographique

La préparation du support cryptographique fait l'objet d'un contrôle de sécurité par l'OCN.
Le stockage et la diffusion du support cryptographique sont sécurisés.
Les données d'activation sont établies de façon sécurisées et diffusées séparément du support cryptographique.

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 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. PROFILS DES CERTIFICATS FINAUX

7.2.1. Personnes_Authentification

Nom	Valeur	
Version	2 (=version 3)	
Serial number	Défini par l'outil sur 20 octets strictement	
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION	
Subject	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OU = <région académique> OU = <académie> (optionnel) OI = SI:FR-110043015 seriaNumber = <email avec @ remplacé par « at »> GN = <Prénom> SN = <Nom> CN = <Prénom> <Nom>	PrintableString UTF8String UTF8String UTF8String UTF8String UTF8String PrintableString UTF8String UTF8String UTF8String
Subject Public Key Info	RSA 2048	
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Validity period	3 years	

Extensions	Critical	Value
Authority Key Identifier	**False**	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	**False**	
Methods of generating key ID		Défini par le logiciel
Key Usage	**True**	
digitalSignature		Set
Certificate Policies	**False**	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.1.1
Basic Constraint	**True**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**False**	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	**False**	
rfc822Name		<Email>
Extended Key Usage	**False**	
clientAuth		Set
Authority Information Access	**False**	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.2.2. Personnes_Authentification_Decrochage

Nom	Valeur	
Version	2 (=version 3)	
Serial number	Défini par l'outil	
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION	
Subject	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OU = <région académique> OU = <académie> (optionnel) OI = SI:FR-110043015 seriaNumber = <email avec @ remplacé par « at »> GN = <Prénom> SN = <Nom> CN = <Prénom> <Nom>	PrintableString UTF8String UTF8String UTF8String UTF8String UTF8String PrintableString UTF8String UTF8String UTF8String
Subject Public Key Info	RSA 2048	
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Validity period	3 years	

Extensions	Critical	Value
Authority Key Identifier	**False**	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	**False**	
Methods of generating key ID		Défini par le logiciel
Key Usage	**True**	
digitalSignature		Set
Certificate Policies	**False**	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.2.1
Basic Constraint	**True**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**False**	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	**False**	
rfc822Name		<Email>
Extended Key Usage	**False**	
clientAuth		Set
Authority Information Access	**False**	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.2.3. Personnes_Chiffrement

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil sur 20 octets strictement
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION
Subject	C = FR PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE UTF8String OU = 0002 110043015 UTF8String OU = <région académique> UTF8String OU = <académie> (optionnel) UTF8String OI = SI:FR-110043015 UTF8String SerialNumber = <email avec @ remplacé par « at »> PrintableString GN = <Prénom> UTF8String SN = <Nom> UTF8String CN = <Prénom> <Nom>UTF8String
Subject Public Key Info	RSA 2048
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Validity period	3 years

Extensions	Critical	Value
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel
Key Usage	True	
keyEncipherment		Set
dataEncipherment		Set
Certificate Policies	False	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.3.1
Basic Constraint	True	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	False	
rfc822Name		<Email>
Extended Key Usage	False	
emailProtection		Set
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.2.4. Personnes_Chiffrement_Matériel

Nom	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil sur 20 octets strictement
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION
Subject	C = FR PrintableString O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE UTF8String OU = 0002 110043015 UTF8String ST = <région académique> UTF8String L = <académie>(optionnel) UTF8String OI = SI:FR-110043015 UTF8String SeriaNumber = <email avec @ remplacé par « at »> PrintableString GN = <Prénom> UTF8String SN = <Nom> UTF8String CN = <givenName> <surname> UTF8String
Subject Public Key Info	RSA 2048
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Validity period	3 years

Extensions	Critical	Value
Authority Key Identifier	False	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	False	
Methods of generating key ID		Défini par le logiciel
Key Usage	True	
keyEncipherment		Set
dataEncipherment		Set
Certificate Policies	False	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.8.1
Basic Constraint	True	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	False	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	False	
rfc822Name		<Email>
Extended Key Usage	False	
emailProtection		Set
Authority Information Access	False	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.2.5. Personnes_Authentification_Matériel

Nom	Valeur	
Version	2 (=version 3)	
Serial number	Défini par l'outil sur 20 octets strictement	
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION	
Subject	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 ST = <région académique> L = <académie>(optionnel) OI = SI:FR-110043015 seriaNumber = <email avec @ remplacé par « at »> GN = <Prénom> SN = <Nom> CN = <Prénom> <Nom>	PrintableString UTF8String UTF8String UTF8String UTF8String UTF8String PrintableString UTF8String UTF8String UTF8String
Subject Public Key Info	RSA 2048	
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Validity period	3 years	

Extensions	Critical	Value
Authority Key Identifier	**False**	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	**False**	
Methods of generating key ID		Défini par le logiciel
Key Usage	**True**	
digitalSignature		Set
Certificate Policies	**False**	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.4.1
Basic Constraint	**True**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**False**	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	**False**	
rfc822Name		<Email>
Extended Key Usage	**False**	
clientAuth		Set
Authority Information Access	**False**	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.2.6. Personnes_Authentification_VSC

Nom	Valeur	
Version	2 (=version 3)	
Serial number	Défini par l'outil sur 20 octets strictement	
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION	
Subject	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OU = CSR : OU[2] OU = CSR : OU[3] OI = SI:FR-110043015 seriaNumber = CSR : SN[0] GN = CSR : GIVENNAME[0] SN = CSR : SURNAME[0] CN = CSR : CN[0]	PrintableString UTF8String UTF8String UTF8String UTF8String UTF8String PrintableString UTF8String UTF8String UTF8String
Subject Public Key Info	RSA 2048	
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Validity period	3 years	

Extensions	Critical	Value
Authority Key Identifier	**False**	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	**False**	
Methods of generating key ID		Défini par le logiciel
Key Usage	**True**	
digitalSignature		Set
Certificate Policies	**False**	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.6.1
Basic Constraint	**True**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**False**	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Subject Alternative Name	**False**	
rfc822Name		<Email>
Extended Key Usage	**False**	
clientAuth		Set
Authority Information Access	**False**	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp

7.3. PROFILS DES LCR

Basic Field	Value
Version	2 (=version 3)
Signature (algorithm & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = 0002 110043015 CN = AUTHENTIFICATION
thisUpdate	AAAA/MM/JJ HH:MM:SS Z (date et heure UTC d'émission de la LCR)
nextUpdate	AAAA/MM/JJ HH:MM:SS Z (date d'émission de la LCR suivante)
revokedCertificates	UserCertificate (numéro de série) RevocationDate (date de révocation)

Extension	Critcal	Value
authorityKeyIdentifier	false	Identique au champ « Subject Key Identifier » du certificat de l'AC
crlNumber	false	Défini par l'outil (séquentiel pour un même client)
issuingDistributionPoint	false	http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
expiredCertsOnCRL	false	Date de création de l'AC Indique la date à partir de laquelle la LCR prend en charge les certificats arrivés à expiration après leur révocation

Caractéristique d'une LCR	Durée de validité : 7 jours Périodicité de mise à jour : 24 heures.

7.4. PROFIL DU CERTIFICAT OCSP_AUTHENTIFICATION

Nom	Valeur	
Version	2 (=version 3)	
Serial number	Défini par l'outil sur 20 octets strictement	
Issuer	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = AC AUTHENTIFICATION	
Subject	C = FR O = MINISTERE DE L'EDUCATION NATIONALE ET DE LA JEUNESSE OU = 0002 110043015 OI = SI:FR-110043015 CN = Signature OCSP - <numéro>	PrintableString UTF8String UTF8String UTF8String UTF8String
Subject Public Key Info	RSA 2048	
Signature (algo. & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)	
Validity period	1 year	

Extensions	Critical	Value
Authority Key Identifier	**False**	
keyIdentifier		Défini par le logiciel
Subject Key Identifier	**False**	
Methods of generating key ID		Défini par le logiciel
Key Usage	**True**	
digitalSignature		Set
Certificate Policies	**False**	
policyIdentifier		1.2.250.1.535.2.2.2.3.1.1.1
policyQualifier-cps		http://igc.pncn.education.gouv.fr/cps
policyIdentifier		1.2.250.1.535.2.2.2.3.6.7.1
Basic Constraint	**True**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**False**	
distributionPoint		http://crl.pncn.education.gouv.fr/AC_AUTHENTIFICATION.crl
Extended Key Usage	**False**	
ocspSigning		Set
Subject Alternative Name	**False**	
Email		support-pncn@education.gouv.fr
Authority Information Access	**False**	
caIssuer		http://igc.pncn.education.gouv.fr/AC_AUTHENTIFICATION.p7b
ocsp		http://ocsp.pncn.education.gouv.fr/AC_AUTHENTIFICATION_ocsp
Extensions	**False**	
OCSP No Check		Configuration Simple

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, de l'AE 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 LCR 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 de porteurs et d'AC
- Les scripts de cérémonies
- Les codes d'activation des supports cryptographiques
- Les journaux d'événements
- La DPC et les procédures internes de l'AC
- Les dossiers d'enregistrement des porteurs
- 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 ; 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 1.5.2, en mentionnant les éléments d'identification suivants : nom, prénom, adresse email ;
- 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 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.

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 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.

9.6.2. Autorité d'enregistrement

Voir paragraphes 1.3.3 et 1.3.4

9.6.3. Porteurs de certificats

En sus des éléments décrits dans le paragraphe 1.3.5, 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.

9.6.4. 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

9.6.5. 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 et des données d'activation du support cryptographique, 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 support cryptographique 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 support cryptographique, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées par le porteur.

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 AUTHENTIFICATION vise une certification aux normes ETSI 319401, ETSI 319411-1.
De plus les profils de certificats qualifiés font l'objet d'une demande de qualification conformément au règlement européen, 910/2014 dit règlement [A2].

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

Les conditions générales d'utilisation [R1] sont diffusées et acceptées par les porteurs au moment de la complétude de leur dossier de demande de certificat.
Une nouvelle version des conditions générales d'utilisation fera apparaître les évolutions afin de faciliter la lecture des nouvelles dispositions par le porteur.

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 »
[A7]	EN 319412-1 « Overview and common data structures »
[A8]	EN 319412-2 « Certificate profile for certificates issued to natural persons »

10.2. DOCUMENTS DE REFERENCE

[R1]	Conditions générales d'utilisation des certificats de la PNCN
[R2]	Politique de Certification de l'AC PNCN

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).