Netheos

Accélérez votre confiance digitale

# AC NETHEOS

# Politique de Certification

# NETHEOS Root CA

| Version | Date | Description | Auteurs | Société |
|---|---|---|---|---|
| 1.0 | 19/05/2020 | Version finale | D.E | Netheos |
| 1.1 | 22/09/2020 | Corrections suite à l'audit | D.E | Netheos |

| Etat du document - Classification | Référence |
|---|---|
| Finalisé - C1 | OID : 1.3.6.1.4.1.55020.1.1.1.1 |

**1 INTRODUCTION ..... 10**

1.1 PRESENTATION GENERALE ..... 10

1.2 IDENTIFICATION DU DOCUMENT ..... 10

1.3 ENTITES INTERVENANT DANS L'IGC ..... 10

*1.3.1 Autorité de certification ..... 10*

*1.3.2 Autorité d'enregistrement ..... 11*

*1.3.3 Porteurs de certificats ..... 11*

*1.3.4 Utilisateurs de certificats ..... 11*

*1.3.5 Autres participants ..... 11*

1.4 USAGE DES CERTIFICATS ..... 12

*1.4.1 Domaines d'utilisation applicables ..... 12*

*1.4.2 Domaines d'utilisation interdits ..... 12*

1.5 GESTION DE LA PC ..... 12

*1.5.1 Entité gérant la PC ..... 12*

*1.5.2 Point de contact ..... 12*

*1.5.3 Entité déterminant la conformité d'une DPC avec la PC ..... 12*

*1.5.4 Procédures d'approbation de la conformité ..... 12*

1.6 DEFINITION ET ACRONYMES ..... 13

*1.6.1 Abréviations ..... 13*

*1.6.2 Définitions ..... 13*

**2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES 15**

2.1 ENTITE CHARGEE DE LA MISE A DISPOSITION DES INFORMATIONS ..... 15

2.2 INFORMATIONS DEVANT ETRE MISES A DISPOSITION ..... 15

2.3 DELAIS ET FREQUENCES DE PUBLICATION ..... 15

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES ..... 16

**3 IDENTIFICATION ET AUTHENTIFICATION ..... 16**

3.1 NOMMAGE ..... 16

*3.1.1 Types de noms ..... 16*

*3.1.2 Nécessité d'utilisation de noms explicites ..... 16*

*3.1.3 Anonymisation ou pseudonymisation des porteurs ..... 16*

*3.1.4 Règles d'interprétation des différentes formes de noms ..... 16*

*3.1.5 Unicité des noms ..... 16*

*3.1.6 Identification, authentification et rôle des marques déposées ..... 16*
3.2 VALIDATION INITIALE DE L'IDENTITE ..... 17
*3.2.1 Méthode pour prouver la possession de la clé privée ..... 17*
*3.2.2 Validation de l'identité d'un organisme ..... 17*
*3.2.3 Validation de l'identité d'un individu ..... 17*
*3.2.4 Informations non vérifiées du porteur ..... 17*
*3.2.5 Validation de l'autorité du demandeur ..... 17*
*3.2.6 Certification croisée d'AC ..... 17*
3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES ..... 17
*3.3.1 Identification et validation pour un renouvellement courant ..... 18*
*3.3.2 Identification et validation pour un renouvellement après révocation ..... 18*
3.4 IDENTIFICATION D'UNE DEMANDE DE REVOCATION ..... 18
**4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS ..... 18**
4.1 DEMANDE DE CERTIFICAT ..... 18
*4.1.1 Origine d'une demande de certificat ..... 18*
*4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat ..... 18*
4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT ..... 18
*4.2.1 Exécution des processus d'identification et de validation de la demande ..... 18*
*4.2.2 Acceptation ou rejet de la demande ..... 18*
*4.2.3 Durée d'établissement du certificat ..... 19*
4.3 DELIVRANCE DU CERTIFICAT ..... 19
*4.3.1 Actions de l'AC concernant la délivrance du certificat ..... 19*
*4.3.2 Notification par l'AC de la délivrance du certificat ..... 19*
4.4 ACCEPTATION DU CERTIFICAT ..... 19
*4.4.1 Démarche d'acceptation du certificat ..... 19*
*4.4.2 Publication du certificat ..... 19*
*4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat ..... 20*
4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT ..... 20
*4.5.1 Usage de la clé privée ..... 20*
*4.5.2 Usage de la clé publique et du certificat ..... 20*
4.6 RENOUVELLEMENT D'UN CERTIFICAT ..... 20
*4.6.1 Causes possibles de renouvellement d'un certificat ..... 20*
*4.6.2 Origine d'une demande de renouvellement ..... 21*

*4.6.3 Procédure de traitement d'une demande de renouvellement ..... 21*
*4.6.4 Notification de l'établissement du nouveau certificat ..... 21*
*4.6.5 Démarche d'acceptation du nouveau certificat ..... 21*
*4.6.6 Publication du nouveau certificat ..... 21*
*4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat ..... 21*
4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE AU CHANGEMENT DE LA BI-CLE ..... 21
*4.7.1 Causes possibles de changement d'une bi-clé ..... 21*
*4.7.2 Origine d'une demande d'un nouveau certificat ..... 21*
*4.7.3 Procédure de traitement d'une demande d'un nouveau certificat ..... 21*
*4.7.4 Notification au porteur de l'établissement du nouveau certificat ..... 22*
*4.7.5 Démarche d'acceptation du nouveau certificat ..... 22*
*4.7.6 Publication du nouveau certificat ..... 22*
*4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat ..... 22*
4.8 MODIFICATION DU CERTIFICAT ..... 22
*4.8.1 Causes possibles de modification d'un certificat ..... 22*
*4.8.2 Origine d'une demande de modification d'un certificat ..... 22*
*4.8.3 Procédure de traitement d'une demande de modification d'un certificat ..... 22*
*4.8.4 Notification au porteur de l'établissement du certificat modifié ..... 22*
*4.8.5 Démarche d'acceptation du certificat modifié ..... 22*
*4.8.6 Publication du certificat modifié ..... 22*
*4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifié ..... 23*
4.9 REVOCATION ET SUSPENSION DES CERTIFICATS ..... 23
*4.9.1 Causes possibles d'une révocation ..... 23*
*4.9.2 Origine d'une demande de révocation ..... 23*
*4.9.3 Procédure de traitement d'une demande de révocation ..... 23*
*4.9.4 Délai accordé au porteur pour formuler la demande de révocation ..... 24*
*4.9.5 Délai de traitement par l'AC d'une demande de révocation ..... 24*
*4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats ..... 24*
*4.9.7 Fréquence d'établissement des LAR ..... 24*
*4.9.8 Délai maximum de publication des LAR/LCR ..... 24*
*4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats ... 24*
*4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats 24*
*4.9.11 Autres moyens disponibles d'information sur les révocations ..... 24*

*4.9.12 Exigences spécifiques en cas de compromission de la clé privée ..... 24*
*4.9.13 Causes possibles d'une suspension ..... 25*
*4.9.14 Origine d'une demande de suspension ..... 25*
*4.9.15 Procédure de traitement d'une demande de suspension ..... 25*
*4.9.16 Limites de la période de suspension d'un certificat ..... 25*
4.10 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS ..... 25
*4.10.1 Caractéristiques opérationnelles ..... 25*
*4.10.2 Disponibilité de la fonction ..... 25*
*4.10.3 Dispositifs optionnels ..... 26*
4.11 FIN DE LA RELATION ENTRE UNE ACO ET L'ACR ..... 26
4.12 SEQUESTRE DE CLE ET RECOUVREMENT ..... 26
*4.12.1 Politique et pratiques de recouvrement par séquestre des clés ..... 26*
*4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session ..... 26*
**5 MESURES DE SECURITE NON TECHNIQUES ..... 26**
5.1 MESURES DE SECURITE PHYSIQUE ..... 26
*5.1.1 Situation géographique et construction des sites ..... 26*
*5.1.2 Accès physique ..... 26*
*5.1.3 Alimentation électrique et climatisation ..... 27*
*5.1.4 Exposition aux dégâts des eaux ..... 27*
*5.1.5 Prévention et protection incendie ..... 27*
*5.1.6 Conservation des supports ..... 27*
*5.1.7 Mise hors service des supports ..... 27*
*5.1.8 Sauvegarde hors site ..... 27*
5.2 MESURES DE SECURITE PROCEDURALES ..... 27
*5.2.1 Rôles de confiance ..... 27*
*5.2.2 Nombre de personnes requises par tâche ..... 31*
*5.2.3 Identification et authentification pour chaque rôle ..... 31*
*5.2.4 Rôles exigeant une séparation des attributions ..... 31*
5.3 MESURES DE SECURITE VIS A VIS DU PERSONNEL ..... 31
*5.3.1 Qualifications, compétences, et habilitations requises ..... 31*
*5.3.2 Procédures de vérification des antécédents ..... 31*
*5.3.3 Exigences en matière de formation initiale ..... 32*
*5.3.4 Exigences en matière de formation continue et fréquences des formations ..... 32*

*5.3.5 Fréquence et séquence de rotations entre différentes attributions ..... 32*
*5.3.6 Sanctions en cas d'actions non autorisées ..... 32*
*5.3.7 Exigences vis à vis du personnel des prestataires externes ..... 32*
*5.3.8 Documentation fournie au personnel ..... 32*
5.4 PROCEDURE DE CONSTITUTION DES DONNEES D'AUDIT ..... 33
*5.4.1 Type d'événements à enregistrer ..... 33*
*5.4.2 Fréquence de traitement des journaux d'événements ..... 33*
*5.4.3 Période de conservation des journaux d'événements ..... 33*
*5.4.4 Protection des journaux d'événements ..... 34*
*5.4.5 Procédure de sauvegarde des journaux d'événements ..... 34*
*5.4.6 Système de collecte des journaux d'événements ..... 34*
*5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement ..... 34*
*5.4.8 Évaluation des vulnérabilités ..... 34*
5.5 ARCHIVAGE DES DONNEES ..... 34
*5.5.1 Types de données à archiver ..... 34*
*5.5.2 Période de conservation des archives ..... 35*
*5.5.3 Protection des archives ..... 35*
*5.5.4 Procédure de sauvegarde des archives ..... 35*
*5.5.5 Exigences d'horodatage des données ..... 35*
*5.5.6 Système de collecte des archives ..... 35*
*5.5.7 Procédure de récupération et de vérification des archives ..... 35*
5.6 CHANGEMENT DE CLE D'AC ..... 36
5.7 REPRISE SUITE A LA COMPROMISSION ET SINISTRE ..... 36
*5.7.1 Procédures de remontée et de traitement des incidents et des compromissions ..... 36*
*5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) ..... 36*
*5.7.3 Procédure de reprise en cas de compromission de la clé privée d'une composante ..... 37*
*5.7.4 Capacités de continuité d'activité suite à un sinistre ..... 37*
5.8 CESSATION D'ACTIVITE AFFECTANT L'AC ..... 37
*5.8.1 Transfert d'activité ou cessation d'activité d'une composante ..... 37*
*5.8.2 Cessation d'activité affectant l'activité AC ..... 37*
**6 MESURES DE SECURITE TECHNIQUES ..... 38**
6.1 GENERATION ET INSTALLATION DE BI-CLES ..... 38
*6.1.1 Génération des bi-clés ..... 38*

*6.1.2 Transmission de la clé privée à son propriétaire ..... 38*
*6.1.3 Transmission de la clé publique à l'AC ..... 38*
6.2 TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS ..... 38
*6.2.1 Tailles des clés ..... 39*
*6.2.2 Vérification de la génération des paramètres des bi-clés et de leur qualité ..... 39*
*6.2.3 Objectifs d'usage de la clé ..... 39*
6.3 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES ..... 39
*6.3.1 Standards et mesures de sécurité pour les modules cryptographiques ..... 39*
*6.3.2 Contrôle de la clé privée par plusieurs personnes ..... 40*
*6.3.3 Séquestre de la clé privée ..... 40*
*6.3.4 Copie de secours de la clé privée ..... 40*
*6.3.5 Archivage de la clé privée ..... 40*
*6.3.6 Transfert de la clé privée vers / depuis le module cryptographique ..... 41*
*6.3.7 Stockage de la clé privée dans un module cryptographique ..... 41*
*6.3.8 Méthode d'activation de la clé privée ..... 41*
*6.3.9 Méthode de désactivation de la clé privée ..... 41*
*6.3.10 Niveau de qualification du module cryptographique et des dispositifs de création de signature . 41*
6.4 AUTRES ASPECTS DE LA GESTION DES BI-CLES ..... 41
*6.4.1 Archivage des clés publiques ..... 41*
*6.4.2 Durées de vie des bi-clés et des certificats ..... 41*
6.5 DONNEES D'ACTIVATION ..... 42
*6.5.1 Génération et installation des données d'activation ..... 42*
*6.5.2 Protection des données d'activation ..... 42*
*6.5.3 Autres aspects liés aux données d'activation ..... 42*
6.6 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES ..... 42
*6.6.1 Exigences de sécurité technique spécifiques aux systèmes informatiques ..... 42*
*6.6.2 Niveau d'évaluation de la sécurité des systèmes informatiques ..... 42*
6.7 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES ..... 43
*6.7.1 Mesures liées à la gestion de la sécurité ..... 43*
*6.7.2 Niveau d'évaluation sécurité du cycle de vie des systèmes ..... 43*
6.8 MESURES DE SECURITE RESEAU ..... 43
6.9 HORODATAGE / SYSTEME DE DATATION ..... 43
**7 PROFILS DE CERTIFICATS ET DES LCR/LAR ..... 43**

7.1 PROFIL DES CERTIFICATS ..... 43
*7.1.1 Certificats de l'ACR ..... 43*
*7.1.2 Certificats de l'AC NETHEOS Swan CA ..... 44*
*7.1.3 Certificats de l'AC NETHEOS Technical CA ..... 45*
7.2 LISTE DE CERTIFICATS REVOQUES ..... 46
*7.2.1 LAR de l'ACR ..... 46*
**8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS ..... 47**
8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS ..... 47
8.2 IDENTITES : QUALIFICATION DES EVALUATEURS ..... 47
8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES ..... 47
8.4 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS ..... 48
8.5 COMMUNICATION DES RESULTATS ..... 48
**9 AUTRES PROBLEMATIQUES METIERS ET LEGALES ..... 48**
9.1 TARIF ..... 48
9.2 RESPONSABILITE FINANCIERE ..... 48
*9.2.1 Couverture par les assurances ..... 48*
*9.2.2 Autres ressources ..... 48*
*9.2.3 Couverture et garantie concernant les entités utilisatrices ..... 49*
9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES ..... 49
*9.3.1 Périmètre des informations confidentielles ..... 49*
*9.3.2 Informations hors du périmètre des informations confidentielles ..... 49*
*9.3.3 Responsabilités en termes de protection des informations confidentielles ..... 49*
9.4 PROTECTION DES DONNEES PERSONNELLES ..... 49
*9.4.1 Politique de protection des données personnelles ..... 49*
*9.4.2 Informations à caractère personnel ..... 49*
*9.4.3 Informations à caractère non personnel ..... 49*
*9.4.4 Responsabilité en termes de protection des données personnelles ..... 50*
*9.4.5 Notification et consentement d'utilisation des données personnelles ..... 50*
*9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives ..... 50*
*9.4.7 Autres circonstances de divulgation d'informations personnelles ..... 50*
9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE ..... 50
9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES ..... 50
*9.6.1 obligations de l'AC ..... 50*

*9.6.2 Obligations de l'autorité d'enregistrement ..... 51*
*9.6.3 Obligations des utilisateurs de certificats ..... 51*
9.7 LIMITE DE GARANTIE ..... 51
9.8 LIMITE DE RESPONSABILITE ..... 51
9.9 INDEMNITES ..... 52
9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA POLITIQUE DE CERTIFICATION ..... 52
*9.10.1 Durée de validité ..... 52*
*9.10.2 Fin anticipée de validité ..... 52*
*9.10.3 Effets de la fin de validité et clauses restant applicables ..... 52*
*9.10.4 Notifications individuelles et communications entre les participants ..... 52*
9.11 AMENDEMENTS A LA POLITIQUE DE CERTIFICATION ..... 52
*9.11.1 Procédures d'amendements ..... 52*
*9.11.2 Mécanisme et période d'information sur les amendements ..... 52*
*9.11.3 Circonstances selon lesquelles l'OID doit être changé ..... 52*
9.12 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS ..... 53
9.13 JURIDICTIONS COMPETENTES ..... 53
9.14 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS ..... 53
9.15 DISPOSITION DIVERSES ..... 53
*9.15.1 Accord global ..... 53*
*9.15.2 Transfert d'activités ..... 53*
*9.15.3 Conséquences d'une clause non valide ..... 53*
*9.15.4 Application et renonciation ..... 53*
9.16 FORCE MAJEURE ..... 53
9.17 AUTRES DISPOSITIONS ..... 54

# 1 INTRODUCTION

## 1.1 PRÉSENTATION GÉNÉRALE

NETHEOS opère une application de type SaaS délivrant un service de souscription numérique à ses clients. Cette application est également évoquée sous le terme Service dans le cadre de ce document.
Afin de compléter son offre, NETHEOS met en place une solution de signature électronique visant la conformité ETSI EN 319411-1 pour le niveau LCP ou NCP+ suivant le processus de délivrance. Le déploiement de cette solution nécessite la mise en œuvre d'une chaine de confiance permettant :

- La mise en œuvre de l'authentification entre tous les acteurs de la solution (serveurs, utilisateurs, administrateurs, etc.) ;
- La signature des documents PDF soumis, soit en mode « cachet serveur » ou en mode « signature utilisateur à base de certificat à la volée ».

Ce document, appelé Politique de Certification (PC), décrit les exigences à respecter par l'Autorité de Certification racine, source de la confiance de la chaîne de confiance NETHEOS.

Techniquement, NETHEOS recourt à une Infrastructure de Gestion des Clés (IGC) :

- hors-ligne pour la gestion de la clé de l'AC Racine (ACR) ;
- en ligne pour la gestion des clés des AC Opérationnelles (ACO).

Lorsque cela n'est pas précisé, le terme « AC » désigne dans le présent document l'AC « NETHEOS Root CA ».

## 1.2 IDENTIFICATION DU DOCUMENT

La présente PC est identifiée par le numéro d'OID suivant : 1.3.6.1.4.1.55020.1.1.1.1

L'organisation de cet OID est la suivante :

- 1.3.6.1.4.1.55020 : Racine d'OID attribuée à NETHEOS
  - .1 : Infrastructure de confiance
    - .1 : Environnement de production
      - .1 : NETHEOS Root CA
        - .1 : Politique de Certification

## 1.3 ENTITÉS INTERVENANT DANS L'IGC

L'AC gère exclusivement des certificats à destination des autorités de certification opérationnelles.

### 1.3.1 AUTORITE DE CERTIFICATION

L'entité en charge de l'AC est NETHEOS.

L'AC met en place un comité de suivi nommé « comité de suivi de l'AC » (C2SAC), sous la responsabilité du responsable des AC NETHEOS. Ce comité est le garant de l'application de la PC et de la bonne concordance avec les autres référentiels documentaires dont notamment la Déclaration des Pratiques de Certification (DPC).

Ce comité est constitué des parties prenantes suivantes :

- Responsable de l'AC ;
- Responsables Sécurité des Systèmes d'Information ;
- Responsable des opérations et communications ;
- Responsable qualité et veille.

L'AC est responsable des certificats signés en son nom et de l'ensemble de l'IGC qu'elle a mise en place.

En particulier, l'AC a la responsabilité des fonctions suivantes :

- la mise en application de la Politique de Certification ;
- l'enregistrement des rôles de confiance et des porteurs de secrets ;
- l'émission des certificats ;
- la gestion du cycle de vie des certificats ;
- l'exploitation de l'IGC ;
- la publication de la Liste des Autorités Révoquées (LAR) et de la Liste des Certificats Révoqués (LCR) ;
- la journalisation et l'archivage des événements et informations relatifs au fonctionnement de l'IGC.

### 1.3.2 AUTORITE D'ENREGISTREMENT

L'AC opère sa propre composante AE pour l'ensemble de la chaîne de confiance.

L'AE assure les fonctions suivantes :

- la production et la validation des dossiers de demande de génération d'un certificat d'AC racine et d'AC opérationnelle ;
- la réception des dossiers de demande de révocation d'un certificat de la chaîne d'AC ;
- la vérification de la légitimité d'une demande de création d'un certificat d'AC (via le C2SAC) ;
- le déclenchement de la génération des certificats dans le cadre d'une cérémonie des clés ;
- le déclenchement de la génération programmée ou ponctuelle des LAR ;
- le déclenchement des fonctions d'archivage des données d'enregistrement des demandes de certificats d'AC, des documents liés aux cérémonies des clés, tout autre document qui doit être conservé pour assurer la traçabilité des actions qui ont lieu autour de la chaîne d'AC.

### 1.3.3 PORTEURS DE CERTIFICATS

Dans le cadre de cette PC, il n'y a pas de porteurs de certificats. Les certificats générés sont ceux des AC qui sont sous la responsabilité du responsable des AC NETHEOS.

### 1.3.4 UTILISATEURS DE CERTIFICATS

Les utilisateurs de certificats sont les clients du service NETHEOS, les services, serveurs et applications qui souhaitent reconnaître les certificats émis par NETHEOS dans le cadre de son service de signature et qui sont rattachées à l'ACR.

### 1.3.5 AUTRES PARTICIPANTS

Sans objet.

## 1.4 USAGE DES CERTIFICATS

### 1.4.1 DOMAINES D'UTILISATION APPLICABLES

#### 1.4.1.1 BI-CLES ET CERTIFICATS DE L'ACR

Les bi-clés et les certificats de l'ACR sont utilisés exclusivement pour la signature :

- des demandes de certificats d'ACO ;
- des LAR.

#### 1.4.1.2 BI-CLES ET CERTIFICATS DES ACO

Les bi-clés et les certificats des ACO sont utilisables exclusivement pour :

- signer des certificats finaux ;
- signer des LCR.

### 1.4.2 DOMAINES D'UTILISATION INTERDITS

Tout autre usage que celui défini au paragraphe précédent est interdit.

## 1.5 GESTION DE LA PC

### 1.5.1 ENTITE GERANT LA PC

La PC est gérée par le C2SAC.

### 1.5.2 POINT DE CONTACT

Toute information concernant la présente PC ou la gestion de l'AC peut être demandée via le point de contact suivant :

| |
|---|
| M. David EMO |
| Poste : Directeur technique |
| Adresse : NETHEOS, Les Centuries I, 93 place Pierre Duhem, 34000 Montpellier |
| Email : hello@netheos.com |
| Téléphone : (+33) 9 72 34 11 80 |

### 1.5.3 ENTITE DETERMINANT LA CONFORMITE D'UNE DPC AVEC LA PC

La conformité de la DPC à la PC est validée par le C2SAC.

### 1.5.4 PROCEDURES D'APPROBATION DE LA CONFORMITE

L'approbation de la conformité est prononcée par le responsable du C2SAC sur la base de résultats d'audits internes et du plan d'action décidé ou validé par ce comité.

Cette approbation est prononcée dans le cadre d'un comité qui en atteste les faits dans un compte rendu. Cela intervient avant la mise en production du service.

## 1.6 DEFINITION ET ACRONYMES

Les acronymes utilisés dans la présente PC sont les suivants :

### 1.6.1 ABREVIATIONS

AC Autorité de Certification

ACO Autorité de Certification Opérationnelle

ACR Autorité de Certification Racine

AE Autorité d'Enregistrement

C2SAC Comité de Suivi de l'AC

CEN Comité Européen de Normalisation

DN Distinguished Name (nom de l'autorité de certification émettrice)

DPC Déclaration des Pratiques de Certification

ETSI European Telecommunications Standards Institute (institut européen des normes de télécommunications)

HSM Hardware Security Module (matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger les clés cryptographiques)

IGC Infrastructure de Gestion de Clés

LAR Liste des Autorités Révoquées

LCR Liste des Certificats Révoqués

OID Object Identifier (identifiant universel d'un objet)

PC Politique de Certification

PP Profil de Protection

PSCo Prestataire de Services de Confiance

RSA Rivest Shamir Adeleman

SSI Sécurité des Systèmes d'Information

### 1.6.2 DEFINITIONS

| | |
|---|---|
| **Authentification** | Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues. |
| **Bi clé** | Une 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** | Donnée sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire de service de certification électronique (PSCE). Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. |
| **Certificat d'AC** | Certificat d'une autorité de certification. |
| **Chaîne de confiance** | Ensemble des certificats nécessaires pour valider la généalogie d'un certificat d'un porteur de certificat.<br>Dans une architecture horizontale simple, la chaîne se compose des certificats suivants :<br>- celui de l'autorité de certification racine, base de la confiance de la chaîne de certification ;<br>- celui de l'autorité de certification qui a émis le certificat ;<br>- celui du porteur de certificat. |
| **HSM** | Boîtier cryptographique matériel dans lequel sont stockées les clés publiques et privées des autorités de certification. |
| **Infrastructure de gestion de clés** | Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc. |
| **Liste de Certificats Révoqués (LCR)** | Liste contenant les identifiants des certificats révoqués ou invalides. |
| **Object Identifier** | Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO (ISO/IEC 9834-1:2012) pour désigner un objet ou une classe d'objets spécifiques. |
| **Produit de sécurité** | Dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité. |
| **Système d'information** | Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par |

| | |
|---|---|
| | ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci. |

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

## 2.1 ENTITE CHARGEE DE LA MISE A DISPOSITION DES INFORMATIONS

Les demandes de publications sont validées par le C2SAC et sont réalisées sous le contrôle du responsable des opérations et de la communication de NETHEOS.

L'entité en charge d'assurer le service de publication est nommé « Service Technique ». L'opération est réalisée par l'Administrateur de l'infrastructure.

## 2.2 INFORMATIONS DEVANT ETRE MISES A DISPOSITION

Sur le périmètre du présent document, les informations publiées sont les suivantes :

- La présente PC ;
- Les LAR ;
- Le certificat auto-signé de l'AC en cours de validité.

La présente PC est publiée au format PDF/A. Les versions obsolètes des éléments définis ci-dessus restent publiées dans un espace dédié du site de publication.

Le lien de publication est le suivant :

- Pour la PC : https://www.netheos.com/politique-denregistrement-politiques-de-certification
- Pour la LAR : http://crl.netheos.com/
- Pour le certificat auto-signé de l'ACR en cours de validité : http://aia.netheos.com/aia/

La DPC n'est pas publiée, tous les éléments publics de la DPC sont intégrés dans la présente PC. La DPC peut être néanmoins consultée après demande auprès du point de contact identifiée au paragraphe 1.5.2.

## 2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les politiques de certification sont remises à jour en cas de changement majeur et a minima tous les deux ans. Elles sont dans les deux cas systématiquement publiées.

Les certificats de l'AC sont diffusés ou mis en ligne préalablement à toute diffusion de certificats d'AC opérationnelles ou de LAR et est mis en ligne 48h maximum après sa génération.

La LAR de l'AC est établie une fois par an en situation normale. Si une révocation d'AC devait intervenir durant l'année, une nouvelle LAR serait générée par anticipation.

En cas de nécessité de révoquer un certificat d'AC opérationnelle, une nouvelle série de LAR est pré-générée et la LAR incluant le certificat nouvellement révoqué est immédiatement publiée. Les suivantes le sont sur le même rythme qu'en situation normale.

## 2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

Les informations publiées sont mises à disposition en lecture à l'ensemble de la communauté des utilisateurs.

Les ajouts, suppressions et modifications sont limités aux seules personnes autorisées de l'AC. L'accès au service de publication se fait de manière nominative et à l'aide d'un moyen d'authentification réunissant au moins 2 facteurs. Seuls les administrateurs de l'entité « Service Technique » peuvent réaliser les opérations de modification sur le service de publication.

# 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), chaque titulaire ayant un nom distinct (DN).

### 3.1.2 NECESSITE D'UTILISATION DE NOMS EXPLICITES

Les noms pour distinguer les certificats sont explicites. Le nom distinctif est conforme à la norme X501 et sous la forme d'une chaîne de type UTF8string.

Si un certificat de test doit être produit en environnement de production, le nom distinctif de ce dernier sera précédé de la chaîne de caractère « TEST ».

### 3.1.3 ANONYMISATION OU PSEUDONYMISATION DES PORTEURS

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes.

Les noms fournis pour l'établissement d'un certificat ne peuvent en aucun cas être des pseudonymes.

### 3.1.4 REGLES D'INTERPRETATION DES DIFFERENTES FORMES DE NOMS

Le nom de l'AC est défini par le C2SAC.

### 3.1.5 UNICITE DES NOMS

Le C2SAC assure l'unicité du DN demandé pour la création du certificat d'AC.

### 3.1.6 IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES

Le C2SAC s'assure au moment de la validation de la demande de certificat d'AC que le nom distinctif utilisé est libre d'utilisation et que la dénomination demandée ne porte pas atteinte à des droits de propriété de tiers.

## 3.2 VALIDATION INITIALE DE L'IDENTITE

Le CS2AC valide directement la demande de certificat d'AC avant le déclenchement de la cérémonie des clés. La demande est faite sous la forme d'un formulaire de demande de création d'AC qui est soumis au CS2AC.

### 3.2.1 METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Le certificat de l'ACR est un certificat auto-signé. La demande technique est générée depuis les interfaces de l'IGC durant la cérémonie des clés.

Un script de cérémonie est produit pour la réalisation de cette cérémonie des clés. Les paramètres de générations sont conformes par rapport au contenu du formulaire de demande de création d'AC.

Un témoin présent lors de la cérémonie des clés atteste du bon déroulé du script de cérémonie. Un procès-verbal est produit à l'issue de cette cérémonie, les formulaires de demandes et les certificats générés sont attestés dans ce Procès-Verbal.

La clé privée de l'ACR est directement générée dans le HSM rattaché à la racine de l'IGC.

Les clés privées des ACO sont directement générées dans le HSM rattaché à l'IGC gérant les ACO.

### 3.2.2 VALIDATION DE L'IDENTITE D'UN ORGANISME

L'organisme porteur des certificats de la chaîne d'AC est NETHEOS. Son identité est validée de fait par le C2SAC lors de l'analyse de la demande de certificat.

### 3.2.3 VALIDATION DE L'IDENTITE D'UN INDIVIDU

La validation de l'identité du demandeur est réalisée dans le cadre du C2SAC.

### 3.2.4 INFORMATIONS NON VERIFIEES DU PORTEUR

La présente PC ne formule pas d'exigence spécifique sur le sujet.

### 3.2.5 VALIDATION DE L'AUTORITE DU DEMANDEUR

La présente version de la PC n'envisage que des émissions de certificats à des AC opérationnelles opérées par NETHEOS.

### 3.2.6 CERTIFICATION CROISEE D'AC

Sans objet.

## 3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

Un nouveau certificat ne peut pas être fourni sans renouvellement de la bi-clé correspondante. Le renouvellement se traduit alors par une nouvelle demande de certificat et bénéficie des mêmes procédures que pour une demande initiale (voir section 3.2 de la présente PC).

### 3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

La procédure est identique à une demande initiale.

### 3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

La procédure est identique à une demande initiale.

## 3.4 IDENTIFICATION D'UNE DEMANDE DE REVOCATION

La demande de révocation de clé pour une AC opérationnelle ne peut émaner que du C2SAC. Elle est validée formellement par le responsable du C2SAC avant prise en compte.

Le certificat de l'ACR étant un certificat auto-signé, il ne peut pas être révoqué. Les certificats des ACO peuvent cependant être révoqués, la décision de révocation étant alors validée par le C2SAC.

En cas de compromission de la clé privée correspondant à un certificat d'AC, le C2SAC réalisera l'ensemble des actions prévues en cas de compromission.

# 4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

## 4.1 DEMANDE DE CERTIFICAT

### 4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

Le demandeur de certificat est le responsable de l'AC. Il réalise la demande directement en complétant et signant le formulaire de demande de certificat d'AC.

### 4.1.2 PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT

Après validation de la demande par le C2SAC, il est planifié une cérémonie des clés au cours de laquelle seront générés les bi-clés et le certificat correspondant. Les opérations techniques se font dans une salle protégée prévue à cet effet.

## 4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

### 4.2.1 EXECUTION DES PROCESSUS D'IDENTIFICATION ET DE VALIDATION DE LA DEMANDE

Le C2SAC reçoit une demande signée du responsable de l'AC.

### 4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

La demande est considérée acceptée si la cérémonie des clés est planifiée et que le script de cérémonie correspondant est produit. En sus le C2SAC formalise la validation dans un compte rendu de son comité.

En cas de rejet de la demande, le C2SAC motive le refus et trace cela dans un compte rendu de son comité.

### 4.2.3 DUREE D'ETABLISSEMENT DU CERTIFICAT

Le C2SAC s'efforce de traiter la demande de certificat dans un délai raisonnable. Même s'il n'y a aucune restriction concernant la durée maximale ou minimale de traitement, un délai maximum de 2 mois est établi entre la validation de la demande par le C2SAC et la réalisation de la cérémonie des clés.

## 4.3 DELIVRANCE DU CERTIFICAT

### 4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Durant la cérémonie des clés, la demande technique est générée. Sa validation par l'IGC de l'ACR déclenche l'opération technique de génération du certificat. Celle-ci contient les actions suivantes :

- génération des bi-clés directement sur les HSM associés à l'IGC (sur le site nominal) ;
- production de la CSR depuis les interfaces de l'IGC ;
- vérification technique de la CSR ;
- soumission de la CSR à l'AC et génération du certificat ;
- vérification du certificat.

Des opérations de réplications de l'environnement cryptographique des ACO est réalisé sur le site secondaire de NETHEOS. Ces opérations de réplication se font également dans le cadre d'une cérémonie des clés, l'environnement cryptographique à répliquer étant nécessairement chiffré durant son transport.

Cette opération de réplication n'est pas nécessairement séquentielle à la génération des clés sur le site nominal.

### 4.3.2 NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT

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

Une fois le certificat validé, il sera publié conformément aux éléments précisés dans le paragraphe 2.3.

## 4.4 ACCEPTATION DU CERTIFICAT

### 4.4.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

L'acceptation du certificat signé par l'AC est consignée sur le procès-verbal de la cérémonie des clés.

### 4.4.2 PUBLICATION DU CERTIFICAT

Le certificat fait l'objet d'une publication sur le site de publication (voir 2.2) avant toute utilisation en production de la clé privée associée.

### 4.4.3 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT

Une fois le certificat validé, il sera publié conformément aux éléments précisés dans le paragraphe 2.3.

## 4.5 USAGE DE LA BI-CLE ET DU CERTIFICAT

### 4.5.1 USAGE DE LA CLE PRIVEE

#### 4.5.1.1 CLE PRIVEE DE L'ACR

La clé privée de l'ACR est utilisée pour :

- signer son propre certificat d'AC (certificat auto-signé) ;
- signer les certificats des AC opérationnelles ;
- signer les LAR.

Ces usages sont explicitement définis dans les extensions des certificats.

#### 4.5.1.2 CLE PRIVEE DES AC OPERATIONNELLES

La clé privée d'une ACO, associée à un certificat émis par l'ACR est destinée à :

- signer les certificats finaux des porteurs ;
- signer la LCR.

Ces usages sont explicitement définis dans les extensions des certificats.

### 4.5.2 USAGE DE LA CLE PUBLIQUE ET DU CERTIFICAT

#### 4.5.2.1 CLE PUBLIQUE ET CERTIFICAT DE L'ACR

Le certificat de l'AC est utilisé pour :

- vérifier l'intégrité de la clé publique de l'AC (certificat auto-signé) ;
- vérifier l'origine et l'intégrité des certificats des AC opérationnelles ;
- vérifier l'origine et l'intégrité des LAR émises.

#### 4.5.2.2 CERTIFICATS DES AC OPERATIONNELLES

Les certificats des ACO émis par l'ACR sont destinés à :

- valider les certificats finaux des porteurs ;
- valider la LCR.

## 4.6 RENOUVELLEMENT D'UN CERTIFICAT

Le renouvellement de certificat, au sens de la RFC 3647, correspondant à la seule modification des dates de validité, n'est pas permis par la présente PC. Seule la délivrance d'un nouveau certificat suite au 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 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet

### 4.6.4 NOTIFICATION DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet

### 4.6.5 DEMARCHE 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 ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

Sans objet

## 4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE AU CHANGEMENT DE LA BI-CLE

Conformément à la [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat lié à la génération d'une nouvelle bi-clé.

### 4.7.1 CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Les bi-clés, et les certificats correspondants de l'ACR, seront renouvelés au minimum tous les 20 ans.

Les bi-clés, et les certificats correspondants des ACO, seront renouvelés au minimum tous les 10 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat (cf. chapitre 4.9.2).

### 4.7.2 ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

La demande d'un nouveau certificat est à l'initiative du C2SAC pour l'ACR et les ACO.

### 4.7.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

La procédure est identique à la demande initiale. L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus. Pour les actions de l'AC, il faut se reporter au chapitre 4.3.1.

### 4.7.4 NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

La procédure est identique à celle à suivre pour la demande initiale.

### 4.7.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

La procédure est identique à celle à suivre pour la demande initiale.

### 4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

La procédure est identique à celle à suivre pour la demande initiale.

### 4.7.7 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU NOUVEAU CERTIFICAT

La procédure est identique à celle à suivre pour la demande initiale.

## 4.8 MODIFICATION DU CERTIFICAT

La modification d'un certificat sans changement de la clé privée n'est pas autorisée. Pour modifier un certificat d'AC, il faut le révoquer puis faire une nouvelle demande.

### 4.8.1 CAUSES POSSIBLES DE MODIFICATION D'UN CERTIFICAT

Sans objet.

### 4.8.2 ORIGINE D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

### 4.8.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

### 4.8.4 NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE

Sans objet.

### 4.8.5 DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE

Sans objet.

### 4.8.6 PUBLICATION DU CERTIFICAT MODIFIE

Sans objet.

### 4.8.7 NOTIFICATION PAR L'AC AUX AUTRES ENTITES DE LA DELIVRANCE DU CERTIFICAT MODIFIE

Sans objet.

## 4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

### 4.9.1 CAUSES POSSIBLES D'UNE REVOCATION

Il peut exister plusieurs causes de révocation de certificat d'une ACO :

- les informations de l'ACO figurant dans son certificat ne sont plus correctes ;
- l'ACO n'a pas respecté les modalités applicables d'utilisation du certificat ;
- l'ACO n'a pas respecté ses obligations découlant de la présente PC ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement de l'ACO ;
- la clé privée de l'ACO est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- le responsable de l'AC demande explicitement la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée et/ou de son support) ;
- cessation d'activité de l'ACO ;
- cessation d'activité de l'ACR.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

### 4.9.2 ORIGINE D'UNE DEMANDE DE REVOCATION

Une demande de révocation de certificat d'ACO ne peut émaner que :

- du responsable du C2SAC ;
- des autorités judiciaires via une décision de justice.

### 4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

Une demande de révocation de certificat réceptionnée par l'AC doit au moins contenir les informations suivantes :

- le numéro de série du certificat à révoquer ;
- le nom associé au certificat à révoquer (DN complet) ;
- le nom et la qualité du demandeur de la révocation ;
- la cause de révocation.

La demande est faite à travers un formulaire prévu à cet effet pour ensuite être signée par le demandeur.

La demande est alors, dès réception, authentifiée et contrôlée par le C2SAC. Le responsable du C2SAC valide la demande et réunit le comité pour organiser au plus tôt une cérémonie des clés afin de traiter techniquement la demande de révocation.

### 4.9.4 DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

Dès que le responsable de l'ACO a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

### 4.9.5 DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION

Le délai maximum de traitement d'une demande de révocation d'un certificat d'ACO est de 72h.

### 4.9.6 EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES UTILISATEURS DE CERTIFICATS

L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état de la chaîne de certificats correspondante jusqu'au certificat de l'ACR. Il pourra utiliser, à cette fin, le dernier statut de révocation publié.

### 4.9.7 FREQUENCE D'ETABLISSEMENT DES LAR

Les LAR sont générées tous les ans.

### 4.9.8 DELAI MAXIMUM DE PUBLICATION DES LAR/LCR

Les LAR sont publiées le plus rapidement possible après la date d'établissement. Au maximum, le délai de publication sera de 30 minutes, prenant en compte le fait qu'il peut y avoir un délai entre le moment de génération de la liste et l'instant où elle est disponible sur le site de publication.

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

Sans objet.

### 4.9.10 EXIGENCES DE VERIFICATION EN LIGNE DE LA REVOCATION DES CERTIFICATS PAR LES UTILISATEURS DE CERTIFICATS

Sans objet.

### 4.9.11 AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

### 4.9.12 EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

En cas de compromission de la clé privée de l'ACR ou d'un certificat d'une ACO, le C2SAC déclenche une réunion de crise et prend les mesures suivantes :

- diffusion auprès des parties prenantes et sur son site de publication de la compromission et alerte sur le fait de ne plus faire confiance aux certificats de la chaîne d'AC concernée,
- organisation d'une cérémonie des clés pour :
  - Si la compromission concerne les clés de l'ACR :
    - révoquer l'ensemble des certificats finaux émis par les ACO ;
    - publier une nouvelle et dernière LCR pour chacune des ACO ;
    - révoquer l'ensemble des certificats des ACO ;
    - réémettre une dernière LAR faisant apparaître les numéros de série des certificats des ACO ;
    - détruire les clés privées de l'ACR.
  - Si la compromission concerne les clés d'une ACO :
    - révoquer l'ensemble des certificats finaux émis par l'ACO ;
    - publier une nouvelle et dernière LCR pour cette ACO ;
    - révoquer le certificat de l'ACO ;
    - publier la nouvelle LAR en cours de validité ;
    - détruire la clé privée de l'ACO.

### 4.9.13 CAUSES POSSIBLES D'UNE SUSPENSION

La suspension de certificats n'est pas autorisée dans la présente PC.

### 4.9.14 ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet.

### 4.9.15 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

### 4.9.16 LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet.

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

### 4.10.1 CARACTERISTIQUES OPERATIONNELLES

NETHEOS fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (jusqu'à et y compris l'ACR). Ces informations permettent également de vérifier les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR ainsi que l'état du certificat de l'AC. Les LCR / LAR sont publiées à l'adresse spécifiée dans le chapitre 2.2, et à l'adresse contenue dans les certificats émis.

### 4.10.2 DISPONIBILITE DE LA FONCTION

La fonction d'information sur l'état des certificats est disponible 24h/24h, 7j/7j. Cette fonction a un taux de disponibilité annuel de 99,95%.

### 4.10.3 DISPOSITIFS OPTIONNELS

Sans objet.

## 4.11 FIN DE LA RELATION ENTRE UNE ACO ET L'ACR

L'ensemble de la chaîne d'AC est sous responsabilité de NETHEOS.

## 4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées des AC ne sont pas séquestrées.

### 4.12.1 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet.

### 4.12.2 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR ENCAPSULATION DES CLES DE SESSION

Sans objet.

# 5 MESURES DE SECURITE NON TECHNIQUES

## 5.1 MESURES DE SÉCURITÉ PHYSIQUE

### 5.1.1 SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES

Les sites d'hébergement des services de confiance hébergeant l'AC respectent les règlements et normes en vigueur (Tiers III) et son installation tient compte des résultats de l'analyse de risques, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques...). Le site d'exploitation (protégé par gardes et des détecteurs d'intrusion, ...) fournit une protection robuste contre les accès non autorisés aux équipements et données de l'AC.

Les hébergeurs sont certifiés ISO27001.

### 5.1.2 ACCES PHYSIQUE

Les équipements de l'AC sont protégés contre les accès non autorisés et les tentatives d'endommagement. La protection physique permet de s'assurer au minimum que :

- La surveillance, manuelle ou électronique, des accès autorisés et non autorisé est assurée ;
- Aucun accès non autorisé ne soit possible sur les équipements sans notification au « Service Technique » ;
- Les supports d'informations papiers et informatiques qui contiennent des informations sensibles en clairs sont stockés dans des endroits sûrs ;
- Les personnes non autorisées soient toujours accompagnées par des personnes autorisées dans les locaux ;
- Un journal des accès soit maintenu ;

- Au moins deux (2) niveaux de barrières de sécurité sont mises en œuvre pour les accès aux équipements ;
- Les systèmes de sécurité physiques (par exemple, des serrures de porte, radars, caméras, ...) sont mis en œuvre ;
- Les locaux sont protégés contre les accès non autorisés.

### 5.1.3 ALIMENTATION ELECTRIQUE ET CLIMATISATION

Le site de type « Tiers III » garantit une redondance de l'alimentation électrique et du système de climatisation.

### 5.1.4 EXPOSITION AUX DEGATS DES EAUX

Les systèmes sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

### 5.1.5 PREVENTION ET PROTECTION INCENDIE

Le site de type « Tiers III » garantit une protection optimale contre les risques d'incendie.

### 5.1.6 CONSERVATION DES SUPPORTS

Les supports (papier et numériques) sont conservés conformément aux procédures définies dans le cadre de l'exploitation de l'AC.

### 5.1.7 MISE HORS SERVICE DES SUPPORTS

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation soit stockés dans un coffre-fort sécurisé.

### 5.1.8 SAUVEGARDE HORS SITE

Les données sont sauvegardées sur un espace dédié de l'hébergeur faisant l'objet d'une offre contractuelle. Cette offre garantit la disponibilité de ces données en cas de survenance d'un sinistre ou d'un événement conduisant à la corruption des données.

NETHEOS dispose également d'un site secondaire, contenant une copie active des données et permettant de répondre aux problématiques d'indisponibilité du site nominal.

## 5.2 MESURES DE SÉCURITÉ PROCÉDURALES

### 5.2.1 ROLES DE CONFIANCE

La structure organisationnelle de l'Infrastructure de Gestion des Clés (IGC) se décline en différentes fonctions :

- Au niveau de l'AC :
  - Représentant légal de l'AC ;
  - Responsable de l'AC ;
  - Responsable de la sécurité des Systèmes d'Information ;
  - Responsable des opérations et communications ;

- Porteurs de secrets (titulaire d'une partie des secrets générés lors de la cérémonie des clés) ;

- Au niveau de l'AE :
  - Responsable AE ;
  - Opérateurs d'enregistrement d'AC ;
  - Opérateurs de révocation ;
- Au niveau du « Service Technique » :
  - Administrateur de l'infrastructure ;
  - Exploitants systèmes et superviseurs ;
  - Auditeur Système ;
- Au niveau de l'organisation transverse :
  - Responsable qualité et veille ;
  - Responsable de l'audit interne des composantes de l'IGC ;
  - Responsable des problématiques juridiques de l'IGC.

Pour chacun de ces rôles, les tâches associées sont les suivantes :

| Fonction | Rôle |
|---|---|
| Responsable d'AC | Le Responsable d'AC préside le comité de suivi et reste responsable des décisions liées à l'AC.<br>Les tâches du responsable d'AC consistent à :<br>• Désigner les porteurs de rôles de confiance (personnes morales et physiques)<br>• S'assurer que les contrats et conventions passés avec les parties prenantes couvrent bien l'intégralité des responsabilités qui leur sont déléguées<br>• Organiser la gestion des secrets de l'AC<br>• Coordonner la rédaction des différentes procédures internes et externes, présentant un impact ou un lien avec des certificats électroniques<br>• Être le référent pour toute demande concernant l'AC<br>• Organiser et à gérer le comité de suivi de l'AC<br>• Déclencher la réalisation des audits de conformité (internes et/ou externes)<br>• Déclencher les processus de qualification des services de confiance |
| Responsable de la sécurité des systèmes d'informations | Il définit les profils d'habilitation physique (droits d'accès, définition des rôles …).<br>Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements |

| | |
|---|---|
| | afin de détecter tout incident, anomalie, tentative de compromission, etc.<br>Le responsable de sécurité est chargé de la définition des règles sécurité établies dans le cadre des politiques et des chartes sécurité.<br>Il est responsable de la définition des profils d'habilitation (droits d'accès, définition des rôles …).<br>Il est responsable de la définition des procédures de gestion des données cryptographiques (Boîtiers cryptographiques, secrets de l'AC).<br>Il est responsable de la mise en œuvre des politiques de sécurité et des chartes sécurité.<br>Il rend compte périodiquement des incidents de sécurité. |
| Responsable des opérations et communications | Il est en charge des équipes opérationnelles de l'IGC. Il est le relais identifié entre les équipes opérationnelles et les instances dirigeantes.<br>Il justifie auprès du responsable d'AC des moyens mis en œuvre pour couvrir les exigences à couvrir au niveau des plateformes de production.<br>Il assure également la veille technique des composants mis en œuvre dans l'infrastructure.<br>Il est également en charge d'organiser la communication autour des services de l'IGC, notamment la communication des incidents de sécurité auprès des clients et des autorités éventuelles |
| Porteur de secrets | Il est responsable d'une part des secrets générés au moment de l'initialisation de l'AC lors de la cérémonie des clés. Les porteurs de secrets n'ont pas forcément de rôles dans les fonctions de l'IGC<br>Il est possesseur d'un support cryptographique contenant une part du secret de l'AC.<br>Un partage de Shamir de 3 parmi 5 est établi pour l'ACR et les ACO. |
| Responsable de l'Autorité d'Enregistrement | Dans ce contexte, il est en charge :<br>• De piloter les phases de développement de ses applicatifs métiers pour leur permettre de s'interfacer avec l'IGC pour gérer les certificats finaux<br>• D'identifier au sein de son organisation les opérateurs d'enregistrements éventuels. |
| Opérateur d'enregistrement d'AC | Il est en charge de valider le contenu des demandes de certificats d'AC. Il s'assure pour cela que les informations portées dans le formulaire de demande de création d'un nouveau certificat d'AC sont justes et il s'assure que la demande a bien été validée et signée par le responsable de l'AC. |

| | |
|---|---|
| | Il participe également à la cérémonie des clés pour assurer les phases de génération technique des demandes de certificats d'AC. |
| Opérateur de révocation | Il s'agit de personnes identifiées au sein de l'organisation de NETHEOS qui peuvent procéder à la révocation d'un certificat final. Des solutions automatisées sont mises en œuvre par NETHEOS pour permettre à un porteur de certificats de révoquer lui-même son certificat, l'opérateur de révocation n'intervient alors que dans le cas où ce processus automatisé n'aurait pas pu aboutir. |
| Administrateur de l'infrastructure | Il est responsable de l'installation, de la sécurisation, de l'évolution et de la configuration des composantes de l'IGC<br>Il est responsable de la mise en œuvre des procédures de sauvegarde et d'archivage.<br>Il est le contact privilégié du responsable sécurité de l'AC. Il est en charge d'assurer le maintien de l'infrastructure en conditions de sécurité.<br>Il décline sur cette infrastructure les règles et procédures de sécurité attendues par l'AC.<br>Il participe aux cérémonies des clés pour réaliser les opérations techniques d'initialisation des HSM, génération des parts de secrets.<br>Il réalise également les opérations sensibles sur les HSM comme les mises à niveau, les sauvegardes, l'externalisation chiffrée des clés. |
| Exploitants systèmes et superviseurs | Il est responsable du suivi opérationnel des composantes de l'IGC<br>Il est responsable de la mise en œuvre des outils de supervision et de gestion des incidents. |
| Auditeur système | Il est responsable de l'analyse récurrente des traces.<br>Il réalise le rapprochement périodique des différentes traces des composantes de l'IGC<br>L'opérateur technique s'assure que la personne responsable de l'analyse des traces n'a pas d'autres fonctions au sein de l'IGC. |
| Responsable juridique | Il est responsable de la validation des parties juridiques détaillées dans le corpus documentaire de l'AC, notamment les PC, CGU et contrats.<br>Il assure également la veille juridique autour de la signature électronique. |
| Responsable de l'audit interne | Il est responsable de la réalisation des audits internes sur les composantes de l'IGC.<br>Il réalise le plan d'audit et s'assure du suivi des plans d'actions établis à la fin des audits. |

| | |
|---|---|
| Responsable qualité et veille | Il est en charge d'assurer la cohérence du référentiel documentaire et assure également le pilotage des audits de certification des services de confiance. |

### 5.2.2 NOMBRE DE PERSONNES REQUISES PAR TACHE

Les tâches dévolues aux différents rôles sont réalisées par au moins une personne. Les rôles sont répartis et gérés (gestion des congés et des arrêts maladie notamment) de manière à assurer une disponibilité constante pour chaque fonction de l'AC.

### 5.2.3 IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE

Pour chacun des membres du personnel ayant accès aux fonctions de l'IGC (opération ou administration), l'identité et les autorisations sont vérifiées avant l'attribution d'un rôle ou des droits correspondants :

- Vérification du membre et ajout à la liste des rôles ;
- Ouverture d'un compte dans les systèmes concernés.

Chaque rôle de confiance signe un formulaire d'acceptance avant la prise de fonction de son rôle.

### 5.2.4 ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. Cependant, pour des raisons de sécurité, certains rôles ne peuvent pas être opérés par la même personne. De façon générale, les rôles et responsabilités sont attribués sur le principe du moindre privilège afin de limiter le risque de conflit d'intérêts et limiter les opportunités de réalisation d'actions non autorisées ou de mauvaise utilisation des biens mis en œuvre par le service de confiance.

Le rôle d'auditeur système ne peut pas être cumulé.

## 5.3 MESURES DE SECURITE VIS A VIS DU PERSONNEL

### 5.3.1 QUALIFICATIONS, COMPETENCES, ET HABILITATIONS REQUISES

Chaque personne amenée à travailler au sein de l'IGC est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles. Les personnels sont formés pour les rôles qu'ils occupent. Les rôles et leurs missions sont documentés afin de bien gérer la séparation des rôles et l'affectation de personne en fonction de la sensibilité des rôles et de leurs compétences, du contrôle des antécédents et de leurs formations.

### 5.3.2 PROCEDURES DE VERIFICATION DES ANTECEDENTS

La société NETHEOS met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de l'IGC. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne

n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions, par la demande d'un extrait du bulletin n°3 du casier judiciaire.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

### 5.3.3 EXIGENCES EN MATIERE DE FORMATION INITIALE

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère. Cette formation couvre les aspects suivants :

- Règles de sécurité ;
- Logiciels de l'IGC en fonction de leur version ;
- Procédures applicables pour les services de de l'IGC ;
- Responsabilités du rôle ;
- Procédures pour la résolution des incidents et des litiges ;
- Connaissance minimale du système informatique de l'IGC ;
- Procédure du plan de continuité.

Le personnel a eu connaissance et compris les implications des opérations dont il a la responsabilité.

### 5.3.4 EXIGENCES EN MATIERE DE FORMATION CONTINUE ET FREQUENCES DES FORMATIONS

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

### 5.3.5 FREQUENCE ET SEQUENCE DE ROTATIONS ENTRE DIFFERENTES ATTRIBUTIONS

La direction de NETHEOS s'assure que les changements de rôles n'affectent pas la sécurité des services de l'IGC.

### 5.3.6 SANCTIONS EN CAS D'ACTIONS NON AUTORISEES

Les sanctions adéquates sont appliquées pour les personnels de l'AC ne respectant pas les règles de sécurité décrite dans la présente PC.

### 5.3.7 EXIGENCES VIS A VIS DU PERSONNEL DES PRESTATAIRES EXTERNES

Il est obligatoire que les prestataires et les visiteurs soient accompagnés par un rôle de confiance de NETHEOS pour avoir accès aux locaux sensibles et aux zones d'hébergement des services de confiance.

Les contrats passés avec des prestataires externes identifient les périmètres d'intervention, les responsabilités, les délais de dépannage, les garanties de qualité et les procédures de traitement d'un incident.

### 5.3.8 DOCUMENTATION FOURNIE AU PERSONNEL

NETHEOS fournit au personnel en charge du service de l'IGC les documentations nécessaires en fonction de leur attribution.

## 5.4 PROCEDURE DE CONSTITUTION DES DONNEES D'AUDIT

### 5.4.1 TYPE D'EVENEMENTS A ENREGISTRER

Les traces des événements suivants sont supposées être directement auditables, sans besoin de rapprochement avec d'autres. Pour cette raison, ils ne sont pas mentionnés dans le présent document. Ces traces sont alors consultables directement sur les équipements concernés. Le responsable de l'AC peut y avoir accès rapidement au travers d'une demande auprès des administrateurs de la plateforme.

Les évènements non concernés par le rapprochement des traces sont :

- Démarrage et arrêt des systèmes informatiques et des applications ;
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- Connexion et déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes ;
- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel.

À l'inverse, les scénarios couvrent les évènements suivants :

- Réception de demande de création de dossier ;
- Visualisation d'un contrat ;
- Validation / rejet d'une demande de certificat ;
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Contrôle automatique d'une pièce justificative ;
- Archivage légal d'un dossier ;
- Acceptation ou rejet d'un dossier client.

### 5.4.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Les journaux d'audits des composantes de l'AC sont revus sur une base trimestrielle par le responsable de l'audit système qui conduit une recherche de preuves d'éventuelles activités malicieuses et de suivi des opérations sensibles.

Le responsable d'audit système explique les événements significatifs dans un rapport d'audit. Une telle revue implique de vérifier que les journaux n'ont pas été altérés, qu'il n'y a pas de discontinuité ou de perte dans les journaux, et par une revue rapide et synthétique de rechercher des incohérences dans les journaux d'audits.

### 5.4.3 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

Les journaux sont accessibles 1 an avant d'être supprimés.

### 5.4.4 PROTECTION DES JOURNAUX D'EVENEMENTS

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'événements. Des mécanismes de contrôle permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les journaux d'événements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

### 5.4.5 PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

Le responsable sécurité met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements, conformément aux exigences de la politique de sécurité. Les sauvegardes des journaux sont protégées avec le même niveau de sécurité que les originaux.

### 5.4.6 SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

Les journaux d'événement sont créés dès la mise en route d'un système et ne s'arrêtent que lorsque le système s'arrête. Le système de collecte des journaux permet de rassembler et de garantir l'intégrité et la disponibilité des journaux d'événement. Si besoin est, le système de collecte des journaux protège les données en intégrité. Si un problème apparait pendant la collecte des journaux, l'exploitant système détermine s'il est nécessaire de suspendre les opérations de la ou des composantes impactées avant d'avoir résolu le problème.

### 5.4.7 NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT

Chacun des événements enregistrés dans le système de collecte des journaux est associé à un serveur ou à un service.

### 5.4.8 ÉVALUATION DES VULNERABILITES

Conformément à nos procédures d'audit, le responsable d'audit est chargé d'analyser les journaux pour détecter toute tentatives frauduleuses. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées.

## 5.5 ARCHIVAGE DES DONNÉES

### 5.5.1 TYPES DE DONNEES A ARCHIVER

L'archivage des données permet d'assurer la pérennité des journaux constitués par l'AE.

Les données archivées au niveau de chaque composante, sont les suivantes :

- Journaux :
- Accès physique (un an) ;
  - Vidéo pour la protection des locaux (un mois) ;
  - Gestion des rôles de confiance (10 ans) ;
  - Accès aux systèmes d'information (5 ans) ;

  - Logs des systèmes d'information et des réseaux (5 ans) ;
  - Documentations de l'AC (5 ans) ;
  - Incident de sécurité et rapports d'audit (10 ans) ;
- Documentation relative à l'audit gardé par l'entité gérant la PC/DPC (5 ans) ;
- Document PC/DPC (5 ans) ;
- Contrat entre NETHEOS et les Clients (5 ans) ;
- Type d'équipement, logiciel et configuration pour l'AC (5 ans) ;
- Autres données et applications utilisés pour la vérification des archives (5 ans) ;
- Tous les journaux relatifs au fonctionnement de l'entité gérant la PE/DPE et des audits (5 ans) ;
- Les dossiers d'enregistrement (7 ans).

### 5.5.2 PERIODE DE CONSERVATION DES ARCHIVES

La période de conservation des archives est donnée au § 5.5.1 ci-dessus.

### 5.5.3 PROTECTION DES ARCHIVES

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- Seront protégées en intégrité, confidentialité et authenticité ;
- Seront accessibles aux seules personnes autorisées ;
- Pourront être consultées et exploitées par les personnes autorisées.

### 5.5.4 PROCEDURE DE SAUVEGARDE DES ARCHIVES

Si les supports utilisés pour le stockage des archives ne peuvent permettre de conserver les données conformément au délai de rétention défini au § 5.5.1, alors un mécanisme de transfert régulier d'archives sur un nouveau support sera mis en œuvre.

### 5.5.5 EXIGENCES D'HORODATAGE DES DONNEES

Les éléments mentionnés au § 5.5.1 ne nécessitent pas d'horodatage fourni par un tiers horodateur. Tous les éléments disposent néanmoins d'un horodatage fourni par le composant sur lequel l'élément a été généré. Tous les composants sont synchronisés sur une même source de temps.

### 5.5.6 SYSTEME DE COLLECTE DES ARCHIVES

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (Se reporter au § 5.4.6).

### 5.5.7 PROCEDURE DE RECUPERATION ET DE VERIFICATION DES ARCHIVES

Les archives sont régulièrement testées afin de s'assurer de leur contenu et de leur lisibilité.

Seules les personnes autorisées et l'entité gérant la PC/DPC peuvent accéder aux archives.

## 5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela, la période de validité du certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement sera demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée sera utilisée pour signer des certificats.

Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

## 5.7 REPRISE SUITE A LA COMPROMISSION ET SINISTRE

### 5.7.1 PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS

Des procédures (sensibilisation, formation des personnels notamment) et des moyens de remontée et de traitement des incidents (analyse des différents journaux d'événements notamment) sont mis en œuvre. En particulier, les anomalies sont remontées automatiquement au « Service Technique ».

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de l'IGC.

Le responsable du C2SAC doit en être informé immédiatement. Il doit alors traiter l'anomalie. S'il estime que l'incident a un niveau de gravité important, il demande une révocation immédiate du certificat. Si celle-ci a lieu, il fait publier l'information de révocation du certificat sous le signe de l'urgence. Il le fait via l'ouverture d'un incident de priorité maximale et via une notification par courrier électronique à l'ensemble des services utilisant les certificats émis par l'AC.

Si l'un des algorithmes ou des paramètres associés, utilisés par l'AC ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors le responsable du C2SAC fait publier l'information via l'ouverture d'un incident et notifie par courrier électronique l'ensemble des services utilisant les certificats émis par l'AC. Tous les certificats concernés sont alors révoqués suivant un planning établi le cas échéant.

### 5.7.2 PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)

Si le matériel de l'AC est endommagé ou hors service alors que les clés de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

En cas de destruction du matériel, l'opérateur technique remplace le matériel défectueux et transmet une copie du procès-verbal de destruction à l'AC.

### 5.7.3 PROCEDURE DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE D'UNE COMPOSANTE

La procédure prévoit notamment à partir de la réception du rapport de suspicion de compromission ou de compromission (source d'information interne ou externe à l'AC) :

- la prise en compte du rapport ;
- la réunion du C2SAC et l'information des intéressés (internes à l'AC) ;
- l'identification de la procédure à appliquer ;
- la mise en œuvre de la procédure à appliquer ;
- l'information des tiers intéressés.

### 5.7.4 CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE

Le PRA est testé annuellement.

## 5.8 CESSATION D'ACTIVITÉ AFFECTANT L'AC

En cas de cessation totale ou partielle d'une activité affectant l'AC, le responsable d'AC préviendra l'organisme ayant délivré les certifications aux services de confiance pour :

- Informer de ce changement,
- Proposer le plan de transfert ou de cessation,
- Etablir la procédure à suivre pour maintenir les certificats de conformité délivré si cela est le souhait de l'AC.

### 5.8.1 TRANSFERT D'ACTIVITE OU CESSATION D'ACTIVITE D'UNE COMPOSANTE

En cas de fin d'activité, l'AC effectue les actions suivantes :

- Notifier les Clients affectés ;
- Transférer les archives à une entité désignée par l'AC permettant de respecter les durées de conservation ;
- Identifier un nouveau responsable de la composante concernée. L'AC s'assure dans ce cas via le C2SAC que ce nouveau responsable assure le bon niveau de sécurité.

### 5.8.2 CESSATION D'ACTIVITE AFFECTANT L'ACTIVITE AC

Afin de permettre au client d'assurer la continuité de ses activités, NETHEOS ainsi que ses prestataires assurent la réversibilité des données en fin de contrat.

Les actions et procédures décrites ci-dessous permettent de garantir la réversibilité :

- Maintien à jour des documentations techniques ou non techniques ;
- Possibilité d'exporter toutes les données du client (base de données, configurations, documents, archives) ;
- Purge des bases de données de NETHEOS ;
- Séquestre du code source à l'agence pour la protection des programmes (APP) ;
- Mise à disposition d'une assistance technique.

# 6 MESURES DE SECURITE TECHNIQUES

## 6.1 GENERATION ET INSTALLATION DE BI-CLES

### 6.1.1 GENERATION DES BI-CLES

#### 6.1.1.1 CLE DE L'ACR

Les clés de l'ACR sont générées lors d'une cérémonie des clés faisant l'objet d'un Procès-Verbal formalisé.

##### 6.1.1.1.1 CEREMONIE DES CLES

La cérémonie de génération des clés se déroule en présence d'un représentant du C2SAC et suivant un script de cérémonie des clés établi par le C2SAC.

##### 6.1.1.1.2 MODULE CRYPTOGRAPHIQUE

Les clés associées aux certificats d'AC sont obligatoirement générées et utilisées dans un module cryptographique ayant fait l'objet d'une qualification par l'ANSSI.

#### 6.1.1.2 CLE DE L'ACO

Les clés de l'ACR sont générées lors d'une cérémonie des clés faisant l'objet d'un Procès-Verbal formalisé.

##### 6.1.1.2.1 CEREMONIE DES CLES

La cérémonie de génération des clés se déroule en présence d'un représentant du C2SAC et suivant un script de cérémonie des clés établi par le C2SAC.

##### 6.1.1.2.2 MODULE CRYPTOGRAPHIQUE

Les clés associées aux certificats d'AC sont obligatoirement générées et utilisées dans un module cryptographique ayant fait l'objet d'une qualification par l'ANSSI.

### 6.1.2 TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE

Les clés privées d'AC sont directement générées dans le module cryptographique correspondant.

### 6.1.3 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La clé publique d'une ACO est transmise dans le cadre d'une cérémonie des clés via un support amovible sécurisé.

## 6.2 TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS

La clé publique d'ACR est enveloppée dans un certificat racine auto signé. Sa diffusion s'accompagne de l'empreinte numérique du certificat ainsi que d'une déclaration précisant qu'il s'agit bien d'une clé publique de l'ACR. La clé publique de l'ACR, ainsi que les

informations correspondantes (certificat, empreinte numérique, déclaration d'appartenance) pourront aisément être récupérées par les utilisateurs de certificats, via l'interface publique (voir 2.2).

### 6.2.1 TAILLES DES CLES

Les clés d'ACR et d'ACO ont les caractéristiques suivantes :

- algorithme utilisé : RSA ;
- taille des clés : 4096 bits.

### 6.2.2 VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE

L'équipement utilisé pour la génération des paramètres des bi-clés des AC est un module cryptographique configuré pour répondre au besoin. Les bi-clés ne peuvent être générées que sur un module cryptographique matériel qualifié.

### 6.2.3 OBJECTIFS D'USAGE DE LA CLE

L'utilisation d'une clé privée d'ACR ou d'ACO et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre 1.4.1).

## 6.3 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

### 6.3.1 STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

#### 6.3.1.1 STANDARDS POUR LES MODULES CRYPTOGRAPHIQUES

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique sécurisé.

Il s'agit d'un module cryptographique Proteccio qualifié par l'ANSSI et fourni par la société ATOS/BULL.

Le boîtier racine est en version EL, ceux de production en version HR.

#### 6.3.1.2 MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

NETHEOS s'assure de la sécurité physique et logicielle des modules cryptographiques utilisés en mettant en œuvre les versions qualifiées de ces équipements. En particulier, NETHEOS s'assure que l'hébergement de ce matériel est dans des zones d'accès contrôlées.

Pour l'ACR, le module cryptographique est hors-ligne et n'est mis en œuvre que dans le cadre de cérémonies des clés.

NETHEOS s'assure de la sécurité des modules cryptographiques tout au long de leur cycle de vie, en particulier, lors de leur mise en place, de la cérémonie des clés et de leur utilisation jusqu'à leur fin de vie.

### 6.3.2 CONTROLE DE LA CLE PRIVEE PAR PLUSIEURS PERSONNES

Le contrôle de la clé privée de signature de l'AC est assuré par du personnel de confiance (porteurs de part de secret) et via un outil mettant en œuvre le partage des secrets.

Il y a N porteurs de part de secret pour chaque AC. Chacun se voit remettre ses parts sur des cartes à puce distinctes lors de la cérémonie des clés. Un quorum de porteurs parmi les N porteurs est nécessaire pour activer la clé privée de l'AC.

### 6.3.3 SEQUESTRE DE LA CLE PRIVEE

Les clés privées des ACR et ACO ne font l'objet d'aucun séquestre.

### 6.3.4 COPIE DE SECOURS DE LA CLE PRIVEE

#### 6.3.4.1 CLE PRIVEE DE L'ACR

La clé privée de l'ACR n'étant pas en permanence activée au sein du module cryptographique, elle fait l'objet d'une copie de secours hors d'un module cryptographique.

Cette copie est réalisée sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et s'appuie notamment sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que la clé privée d'ACR ne soit à aucun moment en clair en dehors du module cryptographique.

Les supports de stockages de la copie de secours sont stockés dans un coffre-fort sur un site différent du site nominal. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.3.2.

#### 6.3.4.2 CLE PRIVEE DES ACO

Les clés privées des ACO sont dupliquées sur le HSM présent sur le site de secours de l'AC. Cette duplication se fait via une copie de secours qui est réalisée sous forme chiffrée avec un mécanisme de contrôle d'intégrité.

Le chiffrement utilisé offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et s'appuie notamment sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée.

Les opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'ACO ne soient à aucun moment en clair en dehors du module cryptographique. Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.3.2.

### 6.3.5 ARCHIVAGE DE LA CLE PRIVEE

Sans objet.

### 6.3.6 TRANSFERT DE LA CLE PRIVEE VERS / DEPUIS LE MODULE CRYPTOGRAPHIQUE

Le transfert vers / depuis le module cryptographique ne se fait que pour la génération des copies de sauvegardes. Ceci se fait sous forme chiffrée, conformément aux exigences du chapitre 6.3.4.

### 6.3.7 STOCKAGE DE LA CLE PRIVEE DANS UN MODULE CRYPTOGRAPHIQUE

Le stockage des clés privées d'AC est réalisé dans un module cryptographique répondant aux exigences du chapitre 6.3.1.

### 6.3.8 METHODE D'ACTIVATION DE LA CLE PRIVEE

L'activation des clés privées d'AC se fait dans un module cryptographique et est contrôlée via des données d'activation.

Pour l'ACR, la clé privée étant désactivée après chaque opération cryptographique (voir 6.3.9), un quorum de porteurs de secrets devra être présent afin de réaliser l'activation de la clé avant chaque opération.

Pour les ACO, l'activation se fait lors de la cérémonie des clés d'initialisation des ACO. Si le HSM contenant les clés des ACO est redémarré, ce redémarrage nécessitera la saisie des données d'activation et nécessitera le quorum des parts de secrets.

### 6.3.9 METHODE DE DESACTIVATION DE LA CLE PRIVEE

Les clés privées des ACR et ACO sont désactivées par arrêt électrique du module cryptographique.

Méthode de destruction des clés privées

La destruction définitive d'une clé privée d'AC est réalisée par :

- la destruction de l'instance de la clé sur le module cryptographique, et
- la destruction des moyens de restauration de la clé privée :
  - la destruction de toutes les copies de secours de la clé privée, ou
  - la destruction des moyens d'activation de la clé privée.

### 6.3.10 NIVEAU DE QUALIFICATION DU MODULE CRYPTOGRAPHIQUE ET DES DISPOSITIFS DE CREATION DE SIGNATURE

Les modules cryptographiques répondent aux exigences du chapitre 6.3.1.

## 6.4 AUTRES ASPECTS DE LA GESTION DES BI-CLES

### 6.4.1 ARCHIVAGE DES CLES PUBLIQUES

Les clés publiques des AC ainsi que les clés publiques incluses dans les certificats émis sont archivées pour la période indiquée au paragraphe 5.5.2.

### 6.4.2 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS

#### 6.4.2.1 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS DE L'ACR

La clé de l'ACR et le certificat associé ont une durée de vie de 20 ans.

#### 6.4.2.2 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS DES ACO

Les clés des ACO et les certificats associés ont une durée de vie maximale de 10 ans.

## 6.5 DONNEES D'ACTIVATION

### 6.5.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

Les éléments nécessaires à l'activation de la clé privée de l'ACR, et des clés privées des ACO sont générés de manière sécurisée, et ne sont accessibles qu'aux seules personnes autorisées à procéder à cette activation.

Ces éléments sont générés dans le cadre de cérémonies des clés et remis à des porteurs de secrets.

### 6.5.2 PROTECTION DES DONNEES D'ACTIVATION

Les parts de secrets sont remises sur une carte à puce qui fait l'objet d'une mise sous enveloppe sécurisée et d'un dépôt dans un coffre sécurisé. Ce coffre est cloisonné pour garantir que seul le porteur de secrets concerné peut accéder aux secrets qui lui sont associés.

### 6.5.3 AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

Sans objet.

## 6.6 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

### 6.6.1 EXIGENCES DE SECURITE TECHNIQUE SPECIFIQUES AUX SYSTEMES INFORMATIQUES

Les exigences de sécurité technique spécifiques aux systèmes informatiques sont décrites dans la politique de sécurité des systèmes d'informations (PSSI) de NETHEOS. Cette politique aborde les objectifs de sécurité suivants :

- Identification et authentification ;
- Contrôle d'accès ;
- Intégrité des composants ;
- Sécurité des flux :
- Journalisation et audits ;
- Supervision et contrôle ;
- Sensibilisation.

### 6.6.2 NIVEAU D'EVALUATION DE LA SECURITE DES SYSTEMES INFORMATIQUES

Des audits sont planifiés par le responsable des audits internes en collaboration avec le responsable de la sécurité.

La fréquence des audits s'établit comme suit :

- Audits tous les ans minimum, diligentés par le responsable de la sécurité du système d'information ;
- Audits ponctuels : en cas de doute, de suspicion, sur le niveau de qualité de la gestion de l'infrastructure interne ou de l'AC.

## 6.7 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

### 6.7.1 MESURES LIEES A LA GESTION DE LA SECURITE

Toute évolution significative d'un système ou d'une composante de l'AC est documentée.

### 6.7.2 NIVEAU D'EVALUATION SECURITE DU CYCLE DE VIE DES SYSTEMES

L'implémentation du système permettant de mettre en œuvre les composantes de l'AC est documentée. La configuration du système de ces composantes ainsi que toute modification et mise à niveau est documentée.

## 6.8 MESURES DE SÉCURITÉ RÉSEAU

Les mesures de sécurité réseau sont décrites dans la politique de sécurité des systèmes d'informations (PSSI) de NETHEOS.

## 6.9 HORODATAGE / SYSTÈME DE DATATION

Pour l'ACR, l'AC étant hors ligne, l'horloge est synchronisée manuellement avant toute utilisation. Cette opération est faite pendant la cérémonie des clés.

Les ACO, quant à elles, sont synchronisées suivant les modalités évoquées au paragraphe 5.5.5.

# 7 PROFILS DE CERTIFICATS ET DES LCR/LAR

## 7.1 PROFIL DES CERTIFICATS

### 7.1.1 CERTIFICATS DE L'ACR

#### 7.1.1.1 CHAMPS DE BASE DU CERTIFICAT

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|---|---|
| **Version** | 2 (pour version 3) |
| **SerialNumber** | Généré automatiquement lors de la cérémonie des clés |
| **Signature** | Sha256WithRSAEncryption |

| | |
|---|---|
| **Issuer** | • CN=NETHEOS Root CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS<br>• C=FR |
| **Subject** | Identique à l'issuer (certificat auto-signé)<br>• CN=NETHEOS Root CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS<br>• C=FR |
| **Validity** | • notBefore: Date de création<br>• notAfter: notBefore + 20 ans |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.1.2 EXTENSIONS DU CERTIFICAT

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---|---|---|---|
| **authorityKeyIdentifier** | 2.5.29.35 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **subjectKeyIdentifier** | 2.5.29.14 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **keyUsage** | 2.5.29.15 | Oui | keyCertSign, CRLSign |
| **basicConstraints** | 2.5.29.19 | Non | • CA: true<br>• Maximum Path Length : absent |
| **authorityInfoAccess** | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: http://aia.netheos.com/aia/rca.crt |

### 7.1.2 CERTIFICATS DE L'AC NETHEOS SWAN CA

#### 7.1.2.1 CHAMPS DE BASE DU CERTIFICAT

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|---|---|
| **Version** | 2 (pour version 3) |
| **SerialNumber** | Généré automatiquement lors de la cérémonie des clés |
| **Signature** | Sha256WithRSAEncryption |
| **Issuer** | • CN=NETHEOS Root CA<br>• orgID=VATFR-78453023681 |

| | |
|---|---|
| | • O=NETHEOS<br>• C=FR |
| **Subject** | • CN=NETHEOS Swan CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS<br>• C=FR |
| **Validity** | • notBefore: Date de création<br>• notAfter: notBefore + 10 ans |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.2.2 EXTENSIONS DU CERTIFICAT

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---|---|---|---|
| **authorityKeyIdentifier** | 2.5.29.35 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **subjectKeyIdentifier** | 2.5.29.14 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **keyUsage** | 2.5.29.15 | Oui | keyCertSign, CRLSign |
| **basicConstraints** | 2.5.29.19 | Non | • CA: true<br>• Maximum Path Length : absent |
| **cRLDistributionPoints** | 2.5.29.31 | Non | Full Name:<br>• URI: http://crl.netheos.com/rca.crl |
| **authorityInfoAccess** | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: http://aia.netheos.com/aia/rca.crt |

### 7.1.3 CERTIFICATS DE L'AC NETHEOS TECHNICAL CA

#### 7.1.3.1 CHAMPS DE BASE DU CERTIFICAT

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|---|---|
| **Version** | 2 (pour version 3) |
| **SerialNumber** | Généré automatiquement lors de la cérémonie des clés |
| **Signature** | Sha256WithRSAEncryption |
| **Issuer** | • CN=NETHEOS Root CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS |

| | |
|---|---|
| | • C=FR |
| **Subject** | • CN=NETHEOS Technical CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS<br>• C=FR |
| **Validity** | • notBefore: Date de création<br>• notAfter: notBefore + 10 ans |
| **Subject Public Key Info** | RSA 4096 bits |

#### 7.1.3.2 EXTENSIONS DU CERTIFICAT

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---|---|---|---|
| **authorityKeyIdentifier** | 2.5.29.35 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **subjectKeyIdentifier** | 2.5.29.14 | Non | [RFC 5280] méthode [1] : identifiant de la clé publique contenue dans le certificat |
| **keyUsage** | 2.5.29.15 | Oui | keyCertSign, CRLSign |
| **basicConstraints** | 2.5.29.19 | Non | • CA: true<br>• Maximum Path Length : absent |
| **cRLDistributionPoints** | 2.5.29.31 | Non | Full Name:<br>• URI: http://crl.netheos.com/rca.crl |
| **authorityInfoAccess** | 1.3.6.1.5.5.7.1.1 | Non | CA Issuers - URI: http://aia.netheos.com/aia/rca.crt |

## 7.2 LISTE DE CERTIFICATS REVOQUES

## 7.2.1 LAR DE L'ACR

#### 7.2.1.1 CHAMPS DE BASE

Le tableau suivant présente les champs de base :

| Champ | Valeur |
|---|---|
| **Version** | 1 (pour version 2) |
| **Signature** | SHA256WithRSA |
| **Issuer** | • CN=NETHEOS Root CA<br>• orgID=VATFR-78453023681<br>• O=NETHEOS<br>• C=FR |

| | |
|---|---|
| **Validity** | 425 jours |
| **Revoked Certificates** | • Serial Number<br>• Revocation Date |

#### 7.2.1.2 EXTENSIONS

Le tableau suivant présente les extensions :

| Champ | OID | Criticité | Valeur |
|---|---|---|---|
| **authorityKeyIdentifier** | 2.5.29.35 | Non | [RFC 5280] méthode [0] : identifiant de la clé publique de l'AC émettrice |
| **cRLNumber** | 2.5.29.20 | Non | Défini par l'outil |

## 8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Pour s'assurer du niveau de sécurité de son infrastructure interne et de l'autorité certification, NETHEOS a mis en place un processus d'audit.

D'autres audits externes seront réalisés, notamment pour obtenir des certifications de conformité aux normes ETSI et sont réalisés par des organismes disposant des accréditations nécessaires à ce type d'évaluation de conformité.

### 8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

La fréquence des audits s'établit comme suit :

- Audits tous les ans minimum, diligentés par le responsable de la sécurité du système d'information ;
- Audits ponctuels : en cas de doute, de suspicion, sur le niveau de qualité de la gestion de l'infrastructure interne ou de l'AC.

### 8.2 IDENTITÉS : QUALIFICATION DES ÉVALUATEURS

L'équipe d'audit système est constituée d'experts internes à la société NETHEOS spécialistes du domaine de la sécurité.

Cette équipe d'audit est constituée de personnes n'ayant pas de fonctions opérationnelles sur les services de confiance.

Ces personnes sont soumises à des obligations de confidentialité, compte tenu des informations qui seront mises à leur disposition lors de ces audits.

Les auditeurs intervenants sont choisis parmi des personnes jugées compétentes en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée. Ils ont un rôle neutre au sein du système d'information en support des services de confiance.

### 8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'auditeur est composée de personnes neutres. Celles-ci n'ont aucune fonction

opérationnelle ou fonction de sécurité sur les composantes qu'ils auditent.

## 8.4 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

Suite à un audit, s'il y a lieu, un plan de correctifs est mis en place. Celui-ci décrit les remarques faites par l'équipe d'audit ou par l'auditeur externe. Pour chacune de ces remarques, une priorité ainsi qu'une date de correction sont attribuées.

A l'issue d'un audit de sécurité, l'équipe d'audit rend à l'AC un avis parmi les suivants : « conforme », « non conforme », « avec réserve ».

Selon l'avis rendu, les conséquences du contrôle sont les suivantes. En cas d'avis :

- non conforme, et selon l'importance des non-conformités relevées, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes ;
- avec réserve, l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus ;
- conforme, l'AC confirme à la composante contrôlée la conformité aux exigences de la PC et de la DPC.

## 8.5 COMMUNICATION DES RÉSULTATS

Les résultats des audits sont mis à la disposition du Client sur demande expresse de ce dernier.

# 9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

## 9.1 TARIF

La production de certificats est comprise dans le service de signature. En tout état de cause l'accès au statut des certificats ne fait l'objet d'aucune contrainte tarifaire.

## 9.2 RESPONSABILITÉ FINANCIÈRE

### 9.2.1 COUVERTURE PAR LES ASSURANCES

L'AC a souscrit une assurance responsabilité civile couvrant les risques liés à son activité professionnelle.

### 9.2.2 AUTRES RESSOURCES

L'AC engage les ressources financières nécessaires pour assurer ses activités et notamment la gestion de la fin de vie d'AC. Cela comprend notamment les ressources permettant de maintenir la publication des statuts des certificats qui ont été émis par l'AC, les certificats et documents (Politiques de Certification et CGU) associés.

### 9.2.3 COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

Sans objet.

## 9.3 CONFIDENTIALITÉ DES DONNÉES PROFESSIONNELLES

### 9.3.1 PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations considérées comme confidentielles sont au moins les suivantes :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC ;
- les données d'activation associées aux clés privées d'AC ;
- tous les secrets de l'IGC ;
- les journaux d'événements des composantes de l'IGC ;
- les formulaires de demande de génération et de révocation d'AC ;
- les causes de révocations.

### 9.3.2 INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Sans objet.

### 9.3.3 RESPONSABILITES EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES

NETHEOS applique des procédures de sécurité pour garantir la confidentialité des informations confidentielles. NETHEOS s'engage à respecter la législation et la réglementation en vigueur sur le territoire français.

## 9.4 PROTECTION DES DONNÉES PERSONNELLES

### 9.4.1 POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES

NETHEOS respecte la législation et la réglementation en vigueur sur le territoire français et notamment le respect du RGPD.

NETHEOS maintient des fiches de registre dans ce contexte.

Le respect de ces obligations est contrôlé par un responsable des données personnelles.

### 9.4.2 INFORMATIONS A CARACTERE PERSONNEL

Les données personnelles sont l'ensemble des informations présentes dans le dossier d'enregistrement d'un certificat d'AC ainsi que les rôles de confiance de l'AC

### 9.4.3 INFORMATIONS A CARACTERE NON PERSONNEL

Sans objet.

### 9.4.4 RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

NETHEOS se conforme au RGPD sur la gestion et la protection des données personnelles.

### 9.4.5 NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

Conformément à la législation et la réglementation en vigueur sur le territoire français, les informations personnelles ne sont pas transmises ou communiquées à des tiers sauf dans les cas d'une procédure judiciaire ou d'une demande émanant de la personne concernée par les données personnelles.

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

Les enregistrements seront mis à disposition aux autorités en cas de réquisition judiciaire.

### 9.4.7 AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

Sans objet.

## 9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

NETHEOS détient tous les droits, titres et intérêts relatifs au Service, y compris tous les droits de propriété intellectuelle qui subsistent dans le Service ou qui sont associés aux systèmes ou aux logiciels mis en place pour opérer le Service.

L'utilisation du Service ne confère au Client ou à l'Utilisateur aucun droit de propriété intellectuelle sur le Service ni sur les contenus auxquels il peut accéder (marques, logos, images, sources informatiques, documentations, etc.).

## 9.6 INTERPRÉTATIONS CONTRACTUELLES ET GARANTIES

L'AC, les Clients et les Utilisateurs sont responsables des dommages occasionnés suite à un manquement à leurs obligations respectives telles que définis dans la présente PC et dans les CGU.

### 9.6.1 OBLIGATIONS DE L'AC

NETHEOS en tant qu'AC s'engage à :

- Respecter la PC/DPC et les CGU ;
- Rendre disponible les CGU à l'Utilisateur avant la signature des Documents Métier ;
- Protéger les données d'activation ;
- À collecter les données et pièces justificatives permettant de valide l'identité de l'Utilisateur ;
- Alerter les Clients en cas d'incident de sécurité ayant des conséquences sur le processus d'enregistrement et de signature ;

- Protéger les données personnelles des Utilisateurs.
- Les pratiques de l'AC en matière d'enregistrement sont non discriminatoires ;
- En cas de cessation définitive du service, l'AC s'engage à archiver les certificats émis, la dernière LCR produite, les journaux des actions sur les certificats et les dossiers de preuves associés aux Clients.

### 9.6.2 OBLIGATIONS DE L'AUTORITE D'ENREGISTREMENT

L'AE est assurée directement par l'AC dans le cadre de cette PC. A ce titre elle s'engage à :

- Vérifier le contenu de la demande de certificat avant sa production en cérémonie des clés ;
- Traiter au plus tôt toute demande de révocation d'un certificat d'AC.

### 9.6.3 OBLIGATIONS DES UTILISATEURS DE CERTIFICATS

Les utilisateurs des certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, de celui du porteur à celui de l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et en contrôler sa validité (dates de validité, statut de révocation).

## 9.7 LIMITE DE GARANTIE

Sans objet.

## 9.8 LIMITE DE RESPONSABILITÉ

L'offre du service est soumise à une obligation de moyens, dans les limites de ce qui est commercialement raisonnable et fait cependant l'objet d'une limitation de garantie.

Sauf tel qu'expressément prévu par la présente PC/DPC ou par les conditions d'utilisation générales, ni NETHEOS, ni ses fournisseurs ou distributeurs, ne font aucune promesse spécifique concernant les services. Par exemple, NETHEOS ne s'engage aucunement concernant le contenu des services, les fonctionnalités spécifiques disponibles par le biais des services, leur fiabilité, leur disponibilité ou leur adéquation à répondre aux besoins du client. NETHEOS fournit le service « en l'état ».

Certaines juridictions n'autorisent pas l'exclusion de certaines garanties, telles que la garantie implicite de qualité marchande, d'adéquation à répondre à un usage particulier et de conformité. Dans les limites permises par la loi, NETHEOS exclut toute garantie.

Dans les limites permises par la loi, NETHEOS, ses fournisseurs et distributeurs, déclinent toute responsabilité pour les pertes de bénéfices, de revenus ou de données, ou les dommages et intérêts indirects, spéciaux, consécutifs, exemplaires ou punitifs.

Dans les limites permises par la loi, la responsabilité totale de NETHEOS, de ses fournisseurs et distributeurs, pour toute réclamation dans le cadre des présentes conditions d'utilisation, y compris pour toute garantie implicite, est limitée au montant que le Client a payé pour utiliser le service.

En aucun cas, NETHEOS, ses fournisseurs et distributeurs ne seront tenus responsables pour toute perte ou dommage qui n'aurait pas été raisonnablement prévisible.

## 9.9 INDEMNITÉS

Sans objet.

## 9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA POLITIQUE DE CERTIFICATION

### 9.10.1 DUREE DE VALIDITE

Cette PC reste en application jusqu'à la publication d'une nouvelle version et jusqu'à la fin de vie du dernier certificat émis sous les conditions de cette PC.

### 9.10.2 FIN ANTICIPEE DE VALIDITE

Cette PC reste en application jusqu'à la publication d'une nouvelle version.

### 9.10.3 EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

Sans objet.

### 9.10.4 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

L'AC met à disposition la nouvelle version de la PC dès qu'elle est validée par le C2SAC.

## 9.11 AMENDEMENTS A LA POLITIQUE DE CERTIFICATION

### 9.11.1 PROCEDURES D'AMENDEMENTS

Le C2SAC révise cette PC au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion du C2SAC.

### 9.11.2 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

Lors de tout changement important de cette PC, l'AC informera les différents acteurs de son intention de modifier sa PC avant de procéder aux changements et en fonction de l'objet de la modification. Cette communication sera réalisée par voie électronique.

### 9.11.3 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC)

intervient dans les exigences de la présente PC applicable à la famille de certificats considérée.

## 9.12 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

En cas de contestation sur l'interprétation ou l'exécution de l'une quelconque des dispositions de la présente PC et au cas où les parties ne parviendraient pas à un accord amiable dans les quarante-cinq (45) jours suivant la survenance du différend sauf à ce que ce délai soit prolongé expressément entre elles, les tribunaux situés dans le ressort de la Cour de Grande Instance de Montpellier seront seuls compétents pour connaître de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou encore opposition sur injonction de payer.

## 9.13 JURIDICTIONS COMPÉTENTES

Se reporter au § 9.12.

## 9.14 CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS

L'AC se conforme à la législation et la réglementation en vigueur sur le territoire français.

Comme évoqué en introduction, l'AC se conforme aux exigences de l'ETSI 319411-1 pour le niveau LCP ou NCP+ suivant le processus de délivrance pour la production des certificats électroniques.

## 9.15 DISPOSITION DIVERSES

### 9.15.1 ACCORD GLOBAL

Sans objet.

### 9.15.2 TRANSFERT D'ACTIVITES

Sans objet.

### 9.15.3 CONSEQUENCES D'UNE CLAUSE NON VALIDE

Sans objet.

### 9.15.4 APPLICATION ET RENONCIATION

Sans objet.

## 9.16 FORCE MAJEURE

NETHEOS ne pourra être tenu pour responsable, ou considéré comme ayant failli aux conditions de la présente PC, pour tout retard ou inexécution, lorsque la cause du retard ou de l'inexécution est liée à un cas de force majeure.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuits, ceux habituellement retenus par la jurisprudence des cours et tribunaux français, en application

de l'article 1148 du Code civil, ainsi que les événements suivants : la guerre, l'émeute, l'incendie, les grèves internes ou externes à l'entreprise, occupation des locaux, intempéries, tremblement de terre, tempête, inondation, dégât des eaux, restrictions légales ou gouvernementales, modifications légales ou réglementaires des formes de commercialisation, épidémie, pandémie, l'absence de fourniture d'énergie, pannes d'électricité, du réseau ou des installations ou réseaux de télécommunications, l'arrêt partiel ou total du réseau Internet et, de manière plus générale, des réseaux de télécommunications privés ou publics, tout incident survenant sur le réseau d'un opérateur tiers les blocages de routes et les impossibilités d'approvisionnement en fournitures et tout autre cas indépendant de la volonté expresse de NETHEOS empêchant l'exécution normale du Service

## 9.17 AUTRES DISPOSITIONS

Sans objet.