AC NETHEOS

Politique de Certification

NETHEOS Swan CA

Version	Date	Description	Auteurs	Société
1.0	19/05/2020	Version finale	D.E	Netheos
1.1	15/06/2020	Corrections	L.J	Netheos
1.2	22/09/2020	Corrections suite à l'audit	D.E	Netheos
1.3	11/02/2022	Correction mineure suite à audit interne	L.J	Netheos
1.4	04/10/2022	Modification de la PC	D.E	Netheos
1.5	15/12/2022	Corrections suite à l'audit	D.E	Netheos
1.6	22/03/2023	Corrections suite à la revue des écarts	D.E	Netheos
1.7	04/10/2024	Modification PC suite ajout profil QCP-l	FDV	Datasure

Etat du document - Classification	Référence
Finalisé - C1	OID : 1.3.6.1.4.1.55020.1.1.2.1

1 INTRODUCTION

1.1 PRÉSENTATION GÉNÉRALE

NAMIRIAL (marque commerciale « NETHEOS ») opère une AC Netheos et 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.

NAMIRIAL dispose d'une AC et d'une solution de signature électronique visant la conformité ETSI EN 319 411-1 pour le niveau LCP ou NCP+ suivant le processus de délivrance, et ETSI EN 319 411-2 pour le niveau QCP-l. 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 ».
- La signature de hash 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 NETHEOS Swan CA, rattachée à l'AC racine NETHEOS Root CA.

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 Swan CA ».

La présente PC couvre le déploiement des certificats finaux identifiés de la manière suivante :

- Certificat de signature de PDF de niveau LCP (processus d'identification à distance) : 1.3.6.1.4.1.55020.1.1.2.4.5
- Certificat de signature de PDF de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.1
- Certificat de signature de hash de niveau LCP (processus d'identification à distance) : 1.3.6.1.4.1.55020.1.1.2.4.8

- Certificat de signature de hash de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.7
- Certificat de cachet de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.3
- Certificat de cachet de hash de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.10
- Certificat de cachet de niveau QCP-l (processus d'identification en face à face physique) : 1.3.6.1.4.1.55020.1.1.2.4.11

1.2 IDENTIFICATION DU DOCUMENT

La présente PC est identifiée par le numéro d'OID suivant : 1.3.6.1.4.1.55020.1.1.2.1

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
      - .2 : NETHEOS Swan CA
        - .1 : Politique de Certification

1.3 ENTITÉS INTERVENANT DANS L'IGC

L'AC gère exclusivement des certificats à destination des clients de NETHEOS, sous la forme d'un certificat de signature généré à la volée ou bien sous la forme d'un cachet mis à disposition du client.

1.3.1 AUTORITE DE CERTIFICATION

L'entité en charge de l'AC est NAMIRIAL sous la marque 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

Les opérations de vérification d'identité, préalables à la délivrance d'un certificat de signature, sont déléguées aux Clients de NETHEOS. Les clients sont alors des Autorités d'Enregistrement Déléguées (voir 1.3.3).

Dans ce cadre l'AE assure les fonctions suivantes :

- Le déclenchement de la génération technique des certificats ;
- Le déclenchement des fonctions d'archivage des données de gestion des certificats pour assurer la traçabilité des actions.

Concernant les certificats de cachets, NETHEOS assure directement le rôle d'AE en gérant un processus de demande depuis son service support.

Dans ce cadre l'AE assure les fonctions suivantes :

- La mise à disposition des formulaires de demande de certificats cachets ;
- La réception des dossiers de demande de création de certificats de cachets et de révocation d'un certificat de cachet ;
- La vérification de la légitimité d'une demande de création de certificats de cachets et notamment le lien entre l'entité morale identifiée dans le certificat et le demandeur ;
- Le déclenchement de la génération des certificats ;
- La gestion de la génération et de la transmission des données d'activation du certificat de cachet ;
- Le déclenchement des fonctions d'archivage des données de gestion des certificats pour assurer la traçabilité des actions.

1.3.3 AUTORITE D'ENREGISTREMENT DELEGUEE

Les Clients de NETHEOS peuvent être identifies comme AED pour gérer au plus proches des porteurs de certificats les opérations de vérification d'identité. Dans ce contexte, le Client de NETHEOS est engagé contractuellement dans ce rôle d'AED et s'engage à assurer les fonctions suivantes :

- La vérification des données d'identité du futur signataire ;
- L'utilisation des interfaces de validation des demandes de signature mises en œuvre par NETHEOS.

1.3.4 PORTEURS DE CERTIFICATS

Les porteurs de certificats sont les signataires utilisant directement ou indirectement (via un Client de NETHEOS) les services de NETHEOS pour signer des opérations. Le certificat du signataire est alors émis à la volée durant l'opération de signature et ne peut être utilisé que dans le cadre de cette opération.

1.3.5 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 la chaîne d'AC de NETHEOS.

1.3.6 AUTRES PARTICIPANTS

1.3.6.1 CLIENTS

Il s'agit des clients disposant d'un contrat de services avec NETHEOS. Suivant le contexte un Client peut être une AED, il s'engage dans ce cas contractuellement à assurer les tâches associées.

1.3.6.2 RESPONSABLE DU CERTIFICAT

Le Responsable du Certificat est une personne chez le Client en charge d'assurer la gestion du certificat de cachet qui va être produit par NETHEOS pour le compte du Client. Ce RC est notamment responsable de :

- Produire le dossier de demande de certificat accompagné des justificatifs attendus ;
- D'activer le certificat de cachet qui sera émis par NETHEOS dans le cas du profil NCP+ ;

- De fournir sa CSR, dans le cas du profil QCP-l ;
- De faire les demandes de révocation le cas échéant ;
- De respecter les exigences qui lui incombent au titre de cette PC.

1.4 USAGE DES CERTIFICATS

1.4.1 DOMAINES D'UTILISATION APPLICABLES

1.4.1.1 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.

1.4.1.2 BI-CLES ET CERTIFICATS DE SIGNATURE

Les bi-clés et les certificats de signature sont utilisables exclusivement pour signer des opérations sur la plateforme de signature mise en œuvre par NETHEOS.

1.4.1.3 BI-CLES ET CERTIFICATS DE CACHET

Les bi-clés et les certificats de cachet sont utilisables exclusivement pour signer au nom du Client des opérations sur la plateforme de signature mise en œuvre par NETHEOS.

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 Général Adjoint, 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
AED	Autorité d'Enregistrement Déléguée
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

RC Responsable de Certificats

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. Dans une architecture horizontale simple, la chaîne se compose des certificats suivants : - celui de l'autorité de certification racine, base de la confiance de la chaîne de certification ; - celui de l'autorité de certification qui a émis le certificat ; - celui du porteur de certificat.
Hash	Représentation numérique unique d'un fichier obtenu grâce à une fonction mathématique dite « fonction de hachage ».
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.
Service	Désigne le service fournit en mode SaaS par NETHEOS pour effectuer des opérations de signature électronique. Le service permet aux signataires de signer des documents et des empreintes de fichiers informatiques au sein d'un Parcours Client. Le service constitue et archive les dossiers d'enregistrement relatifs à l'identification et à l'authentification des Utilisateurs.
Signataire	Il s'agit d'un utilisateur personne physique qui est partie prenante dans un parcours client et qui signe des documents métiers. Il est dans le cadre de cette politique de certification le porteur du certificat de signature.
Sujet et souscripteur	Dans le cadre de cette PC, les notions de souscripteur et de sujet sont confondues. Les obligations des conditions générales d'utilisation de l'AC portent exclusivement sur les sujets.
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 CGUs ;
- Les LCR ;
- Le certificat de l'AC en cours de validité ;
- Le certificat auto-signé de l'ACR 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 et les CGUs : https://www.netheos.com/politique-denregistrement-politiques-de-certification
- Pour la LCR : http://crl.netheos.com/
- Pour les certificats d'AC et le certificat auto-signé de l'ACR en cours de validité : http://aia.netheos.com/aia/{nom du fichier du certificat}

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 finaux ou de LCR et sont mis en ligne 48h maximum après leur génération.

La LCR de l'AC est établie une fois par jour en situation normale et après chaque traitement de révocation.

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. De manière générale, 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.

Les LCR sont publiées automatiquement par la PKI après leur génération. La PKI se connecte sur le service de publication via une authentification par clé.

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.

Les certificats de signature contiennent l'identité du signataire dans les champs givenName, surName et commonName.

Les certificats de cachets contiennent :

- L'identité de la personne morale dans les champs organization et organizationIdentifier
- Le nom distinctif du cachet, validé par le Client, dans le champ commonName

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

L'identité portée dans les certificats est conforme aux justificatifs fournis durant la demande. Si les informations attendues dans les certificats ne correspondent pas aux données contenues dans les justificatifs, la demande de certificat sera rejetée.

3.1.5 UNICITE DES NOMS

Les certificats de signature contiennent l'identifiant de l'opération de signature à laquelle ils sont rattachés. Cet identifiant, associé à la date de signature, garantit l'unicité d'un certificat de signature.

Les certificats de cachets contiennent l'identification d'entreprise dans le nom distinctif. Un champ « serialNumber » unique, basé sur la date de génération, garantit l'unicité du nom.

3.1.6 IDENTIFICATION, AUTHENTIFICATION ET ROLE DES MARQUES DEPOSEES

Dans la mesure du possible l'AE s'assure que le nom demandé dans les certificats de cachets est légitime par rapport à la personne morale concernée.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 METHODE POUR PROUVER LA POSSESSION DE LA CLE PRIVEE

Les clés privées sont générées par l'Infrastructure de Gestion de Clés de NETHEOS. Les bi-clés sont conservées dans cette infrastructure et sont :

- Utilisées directement dans une opération de signature pour les certificats de signature ;

- Activées exclusivement pour le compte du Client dans le cadre d'un certificat cachet. Dans ce cadre, seul le RC peut mettre en œuvre ce certificat dans le cadre d'une opération de signature.

3.2.2 VALIDATION DE L'IDENTITE D'UN CLIENT

L'enregistrement du Client nécessite l'identification de l'entité légale, de la personne physique représentant cette entité et la preuve du rattachement de la personne physique à l'entité.

3.2.2.1 IDENTIFICATION DU CLIENT

L'enregistrement du Client nécessite un document officiel (ou émanant d'une source reconnue) en cours de validité au moment de la demande de certificat attestant de l'existence de l'entité et mentionnant le numéro SIREN de celle-ci (extrait Kbis ou certificat d'identification au répertoire national des entreprises ou inscription au répertoire des métiers, etc).

Une source authentique et fiable doit être utilisé pour procéder à cette vérification de personne morale (infogreffe ou data.inpi.fr).

3.2.2.2 IDENTIFICATION DE LA PERSONNE PHYSIQUE REPRESENTANT LE CLIENT

L'enregistrement du représentant du Client nécessite une copie d'au moins un document d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) de la personne physique représentant l'entité. Ce document doit mentionner l'identité complète de la personne physique incluant le prénom et le nom, la date et le lieu de naissance et un numéro national d'identité reconnu.

L'adresse électronique et le numéro de téléphone sont également requis afin de permettre la communication avec la personne physique.

L'identité du représentant du Client est vérifiée au moment de la demande de certificat.

3.2.2.3 PREUVE DU RATTACHEMENT DE LA PERSONNE PHYSIQUE AU CLIENT

L'enregistrement du Client nécessite un document, signé par le mandataire social ou un de ses délégataires, attestant du rattachement de cette personne au Client et de son habilitation à engager la responsabilité de ce Client.

3.2.2.4 IDENTIFICATION DU RESPONSABLE DE CERTIFICAT DE CACHET

Pour le profil de certificats ayant l'OID 1.3.6.1.4.1.55020.1.1.2.4.3 et 1.3.6.1.4.1.55020.1.1.2.4.10, l'identification initiale du responsable de certificat de cachet s'effectue selon la procédure suivante :

- Recueil et vérification du document d'identité du RC ;
- Recueil et vérification du K-BIS et du lien entre le RC et la personne morale ;
- Vérification de l'identité du demandeur via un appel vidéo.

Pour le profil de certificats ayant l'OID 1.3.6.1.4.1.55020.1.1.2.4.11, l'identification initiale du responsable de certificat de cachet s'effectue selon la procédure suivante :

- Recueil et vérification du document d'identité du RC, avec vérification d'identité en face à face physique
- Recueil et vérification du K-BIS et du lien entre le RC et la personne morale ;

3.2.3 VALIDATION DE L'IDENTITE D'UN SIGNATAIRE

Le processus d'enregistrement mis en œuvre par le Client fait dans tous les cas l'objet d'une relation contractuelle avec le service NETHEOS.

3.2.3.1 A DISTANCE

Si le signataire n'a pas fait l'objet d'une vérification d'identité préalable par le Client, le dossier d'enregistrement comprend :

- Une copie d'au moins un document d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) du signataire ou la preuve de l'utilisation d'un moyen d'authentification issue d'une base de connaissance ou qui s'appuie sur un tiers ayant déjà authentifié le signataire ;
- Ou l'identité complète du signataire incluant le prénom et le nom, la date et le lieu de naissance et un numéro national d'identité reconnu.

La validation des informations d'identification du signataire est réalisée soit :

Pour le profil de certificat ayant l'OID 1.3.6.1.4.1.55020.1.1.2.4.5 et 1.3.6.1.4.1.55020.1.1.2.4.8 (LCP)

- Par un processus automatique de validation du document d'identité ;

Pour le profil de certificat ayant l'OID 1.3.6.1.4.1.55020.1.1.2.4.1, 1.3.6.1.4.1.55020.1.1.2.4.7 (NCP+)

- Par un processus de type « facematch » garantissant que le signataire est bien le propriétaire du document d'identité et apportant une preuve de vie du signataire au moment de la demande de certificat. Ce procédé doit garantir l'absence de rejeu, d'usage de faux ou d'artifice visant à usurper une identité. Ce moyen donne l'équivalence à un face à face physique et a fait l'objet d'une validation par un organisme certificateur au regard de la norme ETSI 319-411-1 ;
- Ou par la délivrance d'une lettre recommandée électronique (« LRE ») par un service qualifié au sens du règlement européen n°910/2014 du 23 juillet 2014 reposant sur l'utilisation d'un moyen d'identification de niveau substantiel reconnu par l'ANSSI ;
- Ou par l'utilisation d'un moyen d'identification de niveau substantiel ou élevé reconnu par l'ANSSI.*

3.2.3.2 EN FACE A FACE

Le Client devra s'assurer du respect des obligations suivantes :

- Identifier et authentifier les signataires lors d'un face-à-face avec l'opérateur d'enregistrement de l'AED en demandant au signataire de présenter au moins un document officiel d'identité en cours de validité (passeport, carte nationale d'identité ou titre de séjour) ;
- Documenter ses règles de vérification des informations du signataire portées sur sa pièce d'identité officielle présentée à l'opérateur d'enregistrement de l'AED et, pour les professionnels seulement, les informations portées dans les justificatifs d'appartenance à une entité légale le cas échéant sa fonction au sein de l'entité légale ;
- Collecter une copie des pièces justificatives de l'identité du signataire ainsi que les données d'authentification ;
- Respecter la présente PC ;
- Informer le signataire de la gestion de ses données personnelles et des conditions générales d'utilisation ;
- Enfin, le Client devra avertir immédiatement NETHEOS pour tout incident de sécurité survenant lors de l'enregistrement.

3.2.3.3 SIGNATAIRE DEJA IDENTIFIE

Si le signataire a déjà fait l'objet d'une vérification d'identité préalable par l'AED, celle-ci doit avoir été réalisée conformément aux règles explicitées dans cette PC en fonction du profil de certificat visé.

L'AED s'engage à imposer aux signataires de l'informer de tout changement relatif à leurs informations d'identité dans les plus brefs délais et à s'assurer que les informations d'identité ont été récoltées et contrôlées depuis moins de vingt-quatre mois (24) mois.

De plus, dans ce cas, le Client doit utiliser un moyen d'authentification permettant de s'assurer que le signataire est bien la personne ayant fait l'objet de la vérification initiale (exemple : utilisation d'un compte protégé par un mot de passe, envoi d'un code unique aléatoire par SMS sur un numéro de téléphone mobile vérifié comme étant celui du signataire, certificat, etc…).

NETHEOS validera que l'identification préalable et les authentifications suivantes sont conformes à la présente PC.

3.2.4 VALIDATION DE L'IDENTITE D'UNE ENTITE LEGALE D'UN SIGNATAIRE

Si le signataire appartient à une entité légale alors l'AED vérifie l'existence de l'entité légale et s'assure que le signataire appartient effectivement à celle-ci.

Le dossier d'enregistrement comprend un document en cours de validité au moment de la demande de certificat attestant de l'existence de l'entité et mentionnant le numéro SIREN de celle-ci (extrait Kbis ou certificat d'identification au répertoire national des entreprises ou inscription au répertoire des métiers, etc) ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'existence de l'organisation.

Le dossier d'enregistrement comprend également un document attestant du rattachement de cette personne à l'entité et de son habilitation à engager la responsabilité de l'entité ou bien le résultat de l'interrogation automatique d'un référentiel officiel attestant de l'habilitation du signataire à représenter l'organisation.

3.2.5 INFORMATIONS NON VERIFIEES DU SIGNATAIRE

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

3.2.6 VALIDATION DE L'AUTORITE DU DEMANDEUR

Pour le certificat de signature, les appels au service NETHEOS ne pouvant s'effectuer qu'au sein d'un parcours client et ceux-ci étant authentifiés techniquement, l'autorité du signataire en lien avec le Client est reconnue comme valide.

Pour les certificats de cachets, ces derniers sont rattachés au compte du Client. La mise en œuvre ne peut se faire que par un RC valide.

3.2.7 CERTIFICATION CROISEE D'AC

Sans objet.

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

Concernant les certificats de signature, ceux-ci sont générés lors de chaque opération de signature, il n'y a pas de renouvellement possible.

Concernant les certificats de cachets, le processus de renouvellement est identique au processus de demande initial, il n'y a pas de renouvellements automatiques.

3.3.1 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT

Sans objet.

3.3.2 IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION

Sans objet.

3.4 IDENTIFICATION D'UNE DEMANDE DE REVOCATION

Pour les certificats de signature, la demande de révocation devra être effectuée par le signataire auprès de l'AED du Client. Le Client (ou éventuellement le signataire directement) transmettra alors la demande de révocation par email (revocation@netheos.com) à NETHEOS. La validation de traitement de la révocation sera alors confirmée via email au signataire. La révocation interviendra au plus tard 24 heures après la réception par NETHEOS de la demande de révocation du signataire.

La révocation d'un certificat de cachet se fait par le RC du Client via l'interface du service support. La validation de traitement de la révocation

sera alors confirmée via le ticket support au signataire. La révocation interviendra au plus tard 24 heures après la réception par NETHEOS de la demande de révocation du signataire. Une procédure de secours via l'email de révocation (revocation@netheos.com) est disponible.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 DEMANDE DE CERTIFICAT

4.1.1 ORIGINE D'UNE DEMANDE DE CERTIFICAT

La demande peut être réalisée par le signataire ou bien par le RC du Client.

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

Le Service recueille les informations suivantes afin de constituer la demande de certificat cachet :

- Le nom, prénom, la date et le lieu de naissance du RC ;
- Le SIREN, la raison sociale et l'adresse de l'organisation rattachée au RC.

Afin de pouvoir contacter le Client ou bien le responsable de l'organisation rattachée au RC, le Service recueille également l'adresse électronique et le numéro de téléphone.

Le RC est déjà identifié auprès du service Support de NETHEOS. Il peut donc faire des demandes de certificats cachets.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Concernant les certificats de signature, cela dépend du processus établi contractuellement avec NETHEOS. Les différents cas possibles sont décrits dans le paragraphe 3.2.3. Le Service vérifie donc :

- L'identité du signataire ;
- Que le signataire a pris connaissance des CGU du Service.

Une fois ces vérifications effectuées, le Service émet la demande de certificat. Le Service conserve une copie des éléments d'identification

présentés sous forme électronique et procède à leur horodatage et à leur archivage.

Concernant les certificats de cachets, le RC se connecte au portail du service support en utilisant les identifiants qui lui ont été remis initialement. Il formule ensuite sa demande en fournissant les éléments suivants :

- Informations sur le RC
  - Nom
  - Prénoms
  - Téléphone
  - Email (nominatif)
  - Date et lieu de naissance
  - Adresse postale de la société
- Informations sur le certificat
  - Common Name souhaité (nom du service applicatif, nom de l'entité organisationnelle)
  - Raison sociale (Nom de la société ou structure administrative tel que noté au K-BIS)
  - Numéro d'enregistrement (TVA intracommunautaire, SIREN, RCS, …)
  - Pays

Les pièces justificatives suivantes font partie de la demande :

- Pour le RC
  - Preuve d'identité (CNI, passeport)
  - Formulaire d'attribution de rôle de responsable de certificats cachets signé par le RC
  - Si le RC n'est pas le représentant légal (RL) : formulaire de nomination de responsable de certificats cachets signé par le RL
- Pour la validation de la raison sociale et du nom du représentant légal
  - K-BIS de moins de 3 mois

Dans le cas du profil QCP-l, il revient au RC de fournir la CSR requise pour la génération du certificat.

4.2.2 ACCEPTATION OU REJET DE LA DEMANDE

Si les processus de validation d'identité sont validés, la demande est acceptée, amenant à la génération du certificat concerné.

En cas de rejet de la demande, le Service en informe le Client en le justifiant.

4.2.3 DUREE D'ETABLISSEMENT DU CERTIFICAT

L'AE s'efforce de traiter la demande de certificat dans un délai raisonnable. Néanmoins, il n'y a aucune restriction concernant la durée maximale de traitement.

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT

Le bi-clé et le certificat associé sont générés, stockés et mis en œuvre par l'AC à travers son IGC, sauf pour le profil de cachet QCP-l où une CSR est transmise par le RC.

Concernant le certificat de signature, celui-ci est généré durant l'opération de signature. Les opérations techniques consistent à :

- Générer un bi-clé sur un environnement cryptographique matériel
- Générer la demande de certificat technique depuis le Service
- Transmettre la demande technique à l'IGC
- Signer la demande technique par le certificat de l'AC
- Affecter le certificat à l'opération de signature du Service pour permettre la signature électronique
- Supprimer le bi-clé à la fin de l'opération de signature

Concernant le certificat de cachet, celui-ci est généré suivant un processus de demande fait par le RC auprès du service support NETHEOS.

Les opérations techniques consistent à :

- Pour le RC, créer un ticket de demande de certificat de cachet
- Pour le service support transmettre le ticket auprès de l'administrateur des services de confiance qui se charge de :
    - Créer le bi-clé sur un environnement cryptographique matériel pour le cachet NCP+
    - Générer la demande technique de certificat (CSR) correspondant aux informations fournies par le RC pour le NCP+, ou bien recevoir tel quel la CSR par le RC pour le profil QCP-l

- Faire signer la demande technique de certificat (CSR) par le certificat de l'AC
- Déclencher la génération d'un code d'activation qui sera transmis par téléphone au RC, dans le cas du profil NCP+

- A réception du code d'activation par le RC :
  - se connecter sur le site support
  - vérifier le contenu du certificat qui lui a été généré
  - compléter le ticket lié à sa demande en fournissant le code d'activation qu'il a reçu
- Si le contenu est validé et le code d'activation correct, l'administrateur des services de confiance active le certificat dans le compte du Client.

4.4 NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT

Le certificat de signature fait partie de l'opération de signature.

Le certificat de cachet est tracé dans le ticket généré par le RC sur le service support.

4.5 ACCEPTATION DU CERTIFICAT

4.5.1 DEMARCHE D'ACCEPTATION DU CERTIFICAT

Pour les certificats de signature, l'acceptation du certificat est implicite lors de la signature du document métier ou bien celle de l'empreinte du fichier informatique.

Pour les certificats de cachet, l'acceptation du certificat est explicite :

- En validant les informations du certificat de signature avant de déclencher la signature au niveau du Service
- En acceptant le contenu du certificat de cachet dans le ticket support associé

Dans le cas du profil QCP-l, un formulaire papier d'acceptation du certificat est signé manuscritement par le RC et renvoyée par voie postale au siège français de NAMIRIAL.

4.5.2 PUBLICATION DU CERTIFICAT

Les certificats finaux ne sont pas publiés.

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

L'AC ne notifie pas d'autres entités pour la délivrance des certificats finaux.

4.6 USAGE DE LA BI-CLE ET DU CERTIFICAT

4.6.1 USAGE DE LA CLE PRIVEE

4.6.1.1 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.

4.6.1.2 CLE PRIVEE DES CERTIFICATS FINAUX

La clé privée d'un certificat de signature est utilisée pour signer les opérations de signature liées au Service.

La clé privée d'un certificat de cachet est utilisée pour appliquer le sceau du Client dans le cadre d'une opération de signature liée au Service.

Dans les deux cas, le keyUsage est positionné à digitalSignature et nonRepudiation.

4.6.2 USAGE DE LA CLE PUBLIQUE ET DU CERTIFICAT

4.6.2.1 CERTIFICATS DES AC OPERATIONNELLES

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

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

4.6.2.2 CERTIFICATS FINAUX

Les certificats de signature permettent de :

- Garantir l'intégrité des données signés ;
- S'assurer de l'identité du signataire ;
- Obtenir la non-répudiation des données signées.

Les certificats de cachet permettent de :

- Garantir l'intégrité des données signés ;
- S'assurer que le cachet est bien lié au Client.

4.7 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.

4.7.1 CAUSES POSSIBLES DE RENOUVELLEMENT D'UN CERTIFICAT

Sans objet

4.7.2 ORIGINE D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet

4.7.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT

Sans objet

4.7.4 NOTIFICATION DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet

4.7.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Sans objet

4.7.6 PUBLICATION DU NOUVEAU CERTIFICAT

Sans objet

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

Sans objet

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

Dans tous les cas, le processus de délivrance d'un nouveau certificat suite au changement de la bi-clé est identique au processus initial.

4.8.1 CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE

Sans objet.

4.8.2 ORIGINE D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Sans objet.

4.8.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE D'UN NOUVEAU CERTIFICAT

Sans objet.

4.8.4 NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT

Sans objet.

4.8.5 DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT

Sans objet.

4.8.6 PUBLICATION DU NOUVEAU CERTIFICAT

Sans objet.

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

Sans objet.

4.9 MODIFICATION DU CERTIFICAT

La modification d'un certificat n'est pas autorisée.

4.9.1 CAUSES POSSIBLES DE MODIFICATION D'UN CERTIFICAT

Sans objet.

4.9.2 ORIGINE D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

4.9.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE MODIFICATION D'UN CERTIFICAT

Sans objet.

4.9.4 NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU CERTIFICAT MODIFIE

Sans objet.

4.9.5 DEMARCHE D'ACCEPTATION DU CERTIFICAT MODIFIE

Sans objet.

4.9.6 PUBLICATION DU CERTIFICAT MODIFIE

Sans objet.

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

Sans objet.

4.10 REVOCATION ET SUSPENSION DES CERTIFICATS

Les profils de certificats suivants ne peuvent pas être révoqués du fait de leur durée de vie inférieure au délai minimal de traitement d'une demande de révocation :

- Certificat de signature de PDF de niveau LCP : 1.3.6.1.4.1.55020.1.1.2.4.5
- Certificat de signature de PDF de niveau NCP+ : 1.3.6.1.4.1.55020.1.1.2.4.1
- Certificat de signature de hash de niveau LCP (processus d'identification à distance) : 1.3.6.1.4.1.55020.1.1.2.4.8
- Certificat de signature de hash de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.7
- Certificat de cachet de niveau NCP+ (processus d'identification en face à face) : 1.3.6.1.4.1.55020.1.1.2.4.3
- Certificat de cachet de niveau QCP-l (processus d'identification en face à face physique) : 1.3.6.1.4.1.55020.1.1.2.4.11

4.10.1 CAUSES POSSIBLES D'UNE REVOCATION

Il peut exister plusieurs causes de révocation de certificat :

- Les informations figurant dans son certificat ne sont plus correctes ;
- Le porteur de certificat n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le Client ou le RC n'a pas respecté ses obligations découlant de la présente PC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;

- La clé privée est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- Le Client demande explicitement la révocation du certificat ;
- 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.

4.10.2 ORIGINE D'UNE DEMANDE DE REVOCATION

Une demande de révocation de certificat de signature ne peut émaner que :

- Du signataire via une demande auprès du Client ;
- Du Client (ou du contact Client identifié contractuellement)
- Du responsable de l'AC ;
- Des autorités judiciaires via une décision de justice.

Une demande de révocation de certificat de cachet ne peut émaner que :

- Du RC ;
- Du Client (ou du contact Client identifié contractuellement)
- Du responsable de l'AC ;
- Des autorités judiciaires via une décision de justice.

4.10.3 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION

Pour les certificats de signature, la procédure est la suivante :

- Transmission par email de la demande de révocation à revocation@netheos.com
- Notification par email du porteur de certificat du traitement de sa demande de révocation, dès réception
- Traitement de la demande par le service support :
    - Si le début de traitement est inférieur à la date d'expiration du certificat :

- La demande est transmise à l'administrateur des services de confiance
- L'administrateur s'authentifie sur les interfaces de l'IGC et saisit la demande de révocation
- Une fois la demande traitée, une nouvelle LCR est publiée

- Si le début de traitement est supérieur à la date d'expiration du certificat, alors la révocation ne peut être réalisée

Pour les certificats de cachet, le processus est le suivant :

- Transmission par le RC via le service support de la demande de révocation
- Notification via le ticket support du RC du traitement de sa demande de révocation, dès réception
- Traitement de la demande par le service support :
  - Identification du demandeur pour s'assurer de sa légitimité
  - La demande est transmise à l'administrateur des services de confiance
  - L'administrateur s'authentifie sur les interfaces de l'IGC et saisit la demande de révocation
  - Une fois la demande traitée, une nouvelle LCR est publiée
  - Le certificat cachet est désactivé au niveau du compte du Client

Un certificat révoqué ne peut revenir à l'état « actif ».

Dans le cas où le service support est indisponible, le RC peut transmettre une demande de révocation à l'adresse email revocation@netheos.com. L'AC prend alors la décision de révoquer ce certificat. Le RC est alors informé par email du traitement de sa demande.

4.10.4 DELAI ACCORDE AU PORTEUR POUR FORMULER LA DEMANDE DE REVOCATION

Dès qu'une des causes possibles de révocation est effective, il doit formuler sa demande de révocation sans délai.

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

Le délai maximum de traitement d'une demande de révocation d'un certificat final est de 24h. Ce délai comprend également la publication des CRL mentionnant le changement d'état du certificat.

Si l'utilisateur ne s'est pas authentifié dans un délai de 24h, sa demande de révocation est rejetée.

Dans le cas d'une compromission de la clé privée, le traitement de la révocation sera accéléré et celle-ci sera traitée en moins de 6 heures.

4.10.6 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.

4.10.7 FREQUENCE D'ETABLISSEMENT DES LCR

Les LCR sont générées tous les jours et après chaque traitement d'une révocation.

4.10.8 DELAI MAXIMUM DE PUBLICATION DES LAR/LCR

Les LCR sont publiées le plus rapidement possible après la date d'établissement. Au maximum, le délai de publication est de 1 heure maximum, 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.

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

Sans objet.

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

Sans objet.

4.10.11 AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS

Sans objet.

4.10.12 EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE

En cas de compromission de la clé privée 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 :
  - 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.

4.10.13 CAUSES POSSIBLES D'UNE SUSPENSION

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

4.10.14 ORIGINE D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.10.15 PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE SUSPENSION

Sans objet.

4.10.16 LIMITES DE LA PERIODE DE SUSPENSION D'UN CERTIFICAT

Sans objet.

4.10.17 ÉTAT D'UN CERTIFICAT REVOQUE

L'état d'un certificat révoqué n'est plus modifiable.

4.11 FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS

4.11.1 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.

4.11.2 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%.

4.11.3 DISPOSITIFS OPTIONNELS

Sans objet.

4.12 FIN DE LA RELATION AVEC LE CLIENT

La fin de relation avec le Client déclenche la fin d'accès au Service. Suivant la situation, le certificat de cachet peut être révoqué ou désactivé (en fonction des relations commerciales avec le Client).

4.13 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées ne sont pas séquestrées.

4.13.1 POLITIQUE ET PRATIQUES DE RECOUVREMENT PAR SEQUESTRE DES CLES

Sans objet.

4.13.2 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 du Client :
  - Responsable AED / Contact Client ;
  - Opérateurs d'enregistrement ;
  - Responsable Certificat.
- 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. Les tâches du responsable d'AC consistent à : • Désigner les porteurs de rôles de confiance (personnes morales et physiques) • S'assurer que les contrats et conventions passés avec les parties prenantes couvrent bien l'intégralité des responsabilités qui leur sont déléguées • Organiser la gestion des secrets de l'AC • Coordonner la rédaction des différentes procédures internes et externes, présentant un impact ou un lien avec des certificats électroniques • Être le référent pour toute demande concernant l'AC • Organiser et à gérer le comité de suivi de l'AC • Déclencher la réalisation des audits de conformité (internes et/ou externes) • 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 …). 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. Le responsable de sécurité est chargé de la définition des règles sécurité établies dans le cadre des politiques et des chartes sécurité. Il est responsable de la définition des profils d'habilitation (droits d'accès, définition des rôles …). Il est responsable de la définition des procédures de gestion des données cryptographiques (Boîtiers cryptographiques, secrets de l'AC). Il est responsable de la mise en œuvre des politiques de sécurité et des chartes sécurité. 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. Il justifie auprès du responsable d'AC des moyens mis en œuvre pour couvrir les exigences à couvrir au niveau des plateformes de production. Il assure également la veille technique des composants mis en œuvre dans l'infrastructure. 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 Il est possesseur d'un support cryptographique contenant une part du secret de l'AC. Un partage de Shamir de 3 parmi 5 est établi pour l'ACR et les ACO.
Responsable de l'Autorité d'Enregistrement Délégué	Dans ce contexte, il s'agit du contact Client de NETHEOS qui est en lien contractuel. Il a en charge au sein de son organisation de : • Mettre en œuvre les processus d'enregistrement qui ont été validés avec NETHEOS • Utiliser les interfaces de validation d'identité mises à disposition par NETHEOS
Opérateur d'enregistrement	Il s'agit de collaborateurs du Client qui sont responsables d'assurer le processus d'enregistrement avec le signataire. Il collecte les justificatifs du signataire et upload ces derniers sur les interfaces de validation d'identité de NETHEOS.
Responsable du Certificat	Il s'agit d'un collaborateur du Client formellement identifié par le représentant légal du Client comme étant en charge d'assurer la gestion des certificats de cachets rattachés au Client.
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 Il est responsable de la mise en œuvre des procédures de sauvegarde et d'archivage. 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. Il décline sur cette infrastructure les règles et procédures de sécurité attendues par l'AC.

	Il participe aux cérémonies des clés pour réaliser les opérations techniques d'initialisation des HSM, génération des parts de secrets. Il réalise également les opérations sensibles sur les HSM comme les mises à niveau, les sauvegardes, l'externalisation chiffrée des clés. Il est également en charge d'assurer les opérations techniques permettant de générer les bi-clés des certificats de cachets. Une fois l'activation par le Client obtenue, il se charge d'activer techniquement le certificat cachet correspondant.
Exploitants systèmes et superviseurs	Il est responsable du suivi opérationnel des composantes de l'IGC 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. Il réalise le rapprochement périodique des différentes traces des composantes de l'IGC 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. 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. 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. Pour les collaborateurs NETHEOS, 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 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 certificat ;
- Transmission des Conditions Générales d'Utilisation ;
- Validation / rejet d'une demande de certificat ;

- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Archivage du dossier de demande de certificat.
-

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 apparaît 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 tentative frauduleuse. 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'AC.

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

- Journaux : 1 an
- Accès physique :
  - 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 (10 ans) ;
  - Documentations de l'AC (5 ans après la fin de vie de l'AC) ;
  - Incident de sécurité et rapports d'audit (10 ans) ;
- Documentation relative à l'audit gardé par l'entité gérant la PC/DPC (5 ans après la fin de validité de la PC) ;
- Document PC/DPC (5 ans après la fin de validité de la PC) ;
- Contrat entre NETHEOS et les Clients (5 ans) ;
- Type d'équipement, logiciel et configuration pour l'AC (5 ans après la fin de vie de l'AC) ;

- Autres données et applications utilisés pour la vérification des archives (5 ans) ;
- Tous les journaux relatifs au fonctionnement de l'entité gérant la PC/DPC et des audits (5 ans) ;
- Les dossiers d'enregistrement de demande de certificat (7 ans après la fin de vie du certificat);
- Les dossiers de révocation de certificat (7 ans après la fin de vie du certificat).

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. Ce mécanisme d'archivage est réalisé :

- Pour les dossiers d'enregistrement des certificats : quotidien ;
- Pour les journaux d'événements : hebdomadaire.

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, toutes les 24 heures, sur une même source de temps UTC.

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.

Note : au moment de la cessation de l'activité de l'AC, le certificat d'AC et les informations de révocation peuvent être non valides en cas de compromission du certificat d'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'ACO

Les clés de l'ACO 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 DES CERTIFICATS FINAUX

Les clés des certificats finaux sont générées :

- Lors d'une opération de signature pour les certificats de signature
- Dans le cadre du traitement d'un ticket support pour les certificats de cachet

Les clés sont obligatoirement générées et utilisées dans un module cryptographique ayant fait l'objet d'une certification FIPS 140-2 niveau 3.

6.1.2 TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE

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

6.1.3 TRANSMISSION DE LA CLE PUBLIQUE A L'AC

La clé publique est transmise par :

- Le Service à l'IGC pour les certificats de signature
- L'administrateur des services de confiance pour les certificats de cachet

6.1.4 TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX UTILISATEURS DE CERTIFICATS

La clé publique de l'AC, 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).

6.1.5 TAILLES DES CLES

Les clés de l'AC ont les caractéristiques suivantes :

- Algorithme utilisé : RSA ;
- Taille des clés : 4096 bits.

Les clés des certificats finaux ont les caractéristiques suivantes :

- Algorithme utilisé : RSA ;
- Taille des clés : 2048 bits.

Sauf pour les profils QCP-L qui ont les caractéristiques suivantes :

- Algorithme utilisé : RSA ;
- Taille des clés : 3072 bits minimum.

Il est convenu que la taille des clés des certificats finaux autre que QCP-l soit revue à la hausse conformément aux préconisations de l'ANSSI, et ce en tout état de cause avant le 31/12/2025.

6.1.6 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 des AC ne peuvent être générées que sur un module cryptographique matériel qualifié.

L'équipement utilisé pour la génération des paramètres des bi-clés des certificats finaux est un module cryptographique configuré pour répondre au besoin. Ces bi-clés sont générées sur des modules cryptographiques certifiés FIPS 140-2 niveau 3. Ce niveau de sécurité est paramétré au moment de l'initialisation de l'équipement.

6.1.7 OBJECTIFS D'USAGE DE LA CLE

Voir chapitre 1.4.1

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

6.2.1 STANDARDS ET MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1.1 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.

Les clés de signature des certificats finaux sont générées et mises en œuvre dans un module cryptographique sécurisé. Il s'agit d'un module cryptographique nShield certifié FIPS 140-2 niveau 3 et fourni par nCipher.

6.2.1.2 MESURES DE SECURITE POUR LES MODULES CRYPTOGRAPHIQUES

NETHEOS s'assure que l'hébergement de ce matériel est dans des zones d'accès contrôlées.

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.

6.2.2 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.

6.2.3 SEQUESTRE DE LA CLE PRIVEE

Les clés privées d'AC ne font l'objet d'aucun séquestre.

6.2.4 COPIE DE SECOURS DE LA CLE PRIVEE

6.2.4.1 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 6.2.2.

6.2.4.2 CLE PRIVEE D'UN CERTIFICAT FINAL

Les clés privées des certificats finaux ne font l'objet d'aucune copie.

6.2.5 ARCHIVAGE DE LA CLE PRIVEE

Sans objet.

6.2.6 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 6.2.4.

6.2.7 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 6.2.1.

6.2.8 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. 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.

Pour les certificats finaux, l'activation se fait par l'envoi d'un code à usage unique au signataire qui lui permet de déclencher l'opération de signature.

6.2.9 METHODE DE DESACTIVATION DE LA CLE PRIVEE

Les clés privées d'AC sont désactivées par arrêt électrique du module cryptographique.

Les certificats de signature ne peuvent pas être désactivés du fait de leur courte durée de vie.

Les certificats de cachet peuvent être désactivés par une opération de l'administrateur des services de confiance qui peut associer ou dissocier un certificat cachet au compte du Client.

6.2.10 METHODE DE DESTRUCTION DES CLES PRIVEES

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.

La destruction définitive d'une clé privée d'un certificat final est réalisée par la destruction du bi-clé directement sur l'équipement cryptographique.

6.2.11 NIVEAU DE QUALIFICATION DU MODULE CRYPTOGRAPHIQUE ET DES DISPOSITIFS DE CREATION DE SIGNATURE

Les modules cryptographiques répondent aux exigences du chapitre 6.2.1.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 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.

6.3.2 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS

6.3.2.1 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.

6.3.2.2 DUREES DE VIE DES BI-CLES ET DES CERTIFICATS FINAUX

Les certificats de signature ont une durée de vie de : 60 minutes maximum.

Les certificats de cachet ont une durée de vie de : 2 ans.

6.4 DONNEES D'ACTIVATION

6.4.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION

Les éléments nécessaires à l'activation 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.

Les éléments nécessaires à l'activation des clés privées des certificats finaux sont générés à chaque opération de signature par le Service.

6.4.2 PROTECTION DES DONNEES D'ACTIVATION

Pour le certificat d'ACO, 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.

Pour les certificats finaux, le code à usage unique est transmis directement et exclusivement au signataire.

6.4.3 AUTRES ASPECTS LIES AUX DONNEES D'ACTIVATION

Sans objet.

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1 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.

6.5.2 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 biannuel interne, diligentés par le responsable de la sécurité du système d'information ou son délégué ;
- En alternance avec l'audit biannuel interne, un audit de certification biannuel (jamais la même année) ;
- Audits ponctuels : en cas de doute, de suspicion, sur le niveau de qualité de la gestion de l'infrastructure interne ou de l'AC.

6.6 MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES

6.6.1 MESURES LIEES A LA GESTION DE LA SECURITE

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

6.6.2 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.

6.7 MESURES DE SÉCURITÉ RÉSEAU

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

6.8 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'AC NETHEOS SWAN CA

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 • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Subject	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Validity	• notBefore: Date de création • notAfter: notBefore + 10 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 • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • 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

7.1.2 CERTIFICATS DE SIGNATURE POUR PDF

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 création du certificat
Signature	Sha256WithRSAEncryption
Issuer	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Subject	Pour un signataire entreprise : • C=<Pays de la résidence ou de l'adresse de l'organisation>

	• O=<Organisation du signataire> • OU=< EndUserNCPP|EndUserLCP|EndUserSMPL> • oID=<Identifiant de l'organisation du signataire> • givenName=<Prénom> • surName=<Nom> • CN=<Prénom> <Nom> • serialNumber=<date de signature suivi de l'identifiant unique de l'opération de signature> Pour un signataire particulier : • C=<Pays d'enregistrement de l'autorité de certification> • OU=< EndUserNCPP|EndUserLCP|EndUserSMPL> • givenName=<Prénom> • surName=<Nom> • CN=<Prénom> <Nom> • serialNumber=<date de signature suivie de l'identifiant unique de l'opération de signature>
Validity	• notBefore: Date de création – 1 minute • notAfter: notBefore + 10 minutes
Subject Public Key Info	RSA 2048 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	digitalSignature, nonRepudiation
basicConstraints	2.5.29.19	Non	• CA: False • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI: http://crl.netheos.com/sca.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI: http://aia.netheos.com/aia/sca.crt
extendedKeyUsage	2.5.29.37	Non	PDF Signing ; MS Document Signing
certificatePolicies		Non	policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.4.5 (Certificat de signature de niveau LCP de PDF - processus d'identification à distance) 1.3.6.1.4.1.55020.1.1.2.4.1 (Certificat de signature de niveau NCP+ de PDF - processus d'identification en face à face) policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.1 policyQualifiers = https://www.netheos.com/politique-denregistrement-politiques-de-certification

7.1.3 CERTIFICATS DE SIGNATURE DE HASH

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 création du certificat

Signature	Sha256WithRSAEncryption
Issuer	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Subject	Pour un signataire entreprise : • C=<Pays de la résidence ou de l'adresse de l'organisation> • O=<Organisation du signataire> • OU=<EndUserNCPP|EndUserLCP|EndUserSMPL> • oID=<Identifiant de l'organisation du signataire> • givenName=<Prénom> • surName=<Nom> • CN=<Prénom> <Nom> • serialNumber=<date de signature suivi de l'identifiant unique de l'opération de signature> Pour un signataire particulier : • C=<Pays d'enregistrement de l'autorité de certification> • OU=< EndUserNCPP|EndUserLCP|EndUserSMPL> • givenName=<Prénom> • surName=<Nom> • CN=<Prénom> <Nom> • serialNumber=<date de signature suivie de l'identifiant unique de l'opération de signature>
Validity	• notBefore: Date de création – 1 minute • notAfter: notBefore + 60 minutes (Durée maximale)
Subject Public Key Info	RSA 2048 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	digitalSignature, nonRepudiation
basicConstraints	2.5.29.19	Non	• CA: False • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI: http://crl.netheos.com/sca.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI: http://aia.netheos.com/aia/sca.crt
extendedKeyUsage	2.5.29.37	Non	
certificatePolicies		Non	policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.4.8 (Certificat de signature de niveau LCP de hash - processus d'identification à distance) 1.3.6.1.4.1.55020.1.1.2.4.7 (Certificat de signature de niveau NCP+ de hash - processus d'identification en face à face) policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.1 policyQualifiers = https://www.netheos.com/politique-denregistrement-politiques-de-certification

7.1.4 CERTIFICATS DE CACHETS POUR PDF

7.1.4.1 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 création du certificat
Signature	Sha256WithRSAEncryption
Issuer	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Subject	• C=<Pays d'enregistrement de l'autorité de certification> • O=<Organisation de la personne morale représentée par le cachet> • OU=ServerSeal • OI=<Identifiant d'organisation de la personne morale représentée par le cachet> • CN=Nom du cachet • serialNumber=<date de la création du certificat>
Validity	• notBefore: Date de création – 1 minute • notAfter: notBefore + 2 ans
Subject Public Key Info	RSA 2048 bits

7.1.4.2 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	digitalSignature
basicConstraints	2.5.29.19	Non	• CA: False • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI: http://crl.netheos.com/sca.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI: http://aia.netheos.com/aia/sca.crt
extendedKeyUsage	2.5.29.37	Non	PDF Signing ; MS Document Signing
certificatePolicies		Non	policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.4.3 (Certificat de cachet de niveau NCP+ - processus d'identification en face à face) policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.1 policyQualifiers = https://www.netheos.com/politique-denregistrement-politiques-de-certification

7.1.5 CERTIFICATS DE CACHETS DE HASH

7.1.5.1 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 création du certificat
Signature	Sha256WithRSAEncryption
Issuer	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS

	• C=FR
Subject	• C=<Pays d'enregistrement de l'autorité de certification> • O=<Organisation de la personne morale représentée par le cachet> • OU=ServerSeal • OI=<Identifiant d'organisation de la personne morale représentée par le cachet> • CN=Nom du cachet • serialNumber=<date de la création du certificat>
Validity	• notBefore: Date de création – 1 minute • notAfter: notBefore + 2 ans
Subject Public Key Info	RSA 2048 bits

7.1.5.2 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	digitalSignature
basicConstraints	2.5.29.19	Non	• CA: False • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI: http://crl.netheos.com/sca.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI: http://aia.netheos.com/aia/sca.crt
extendedKeyUsage	2.5.29.37	Non	

certificatePolicies	Non	policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.4.10 (Certificat de cachet de niveau NCP+ - processus d'identification en face à face) policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.1 policyQualifiers = https://www.netheos.com/politique-denregistrement-politiques-de-certification

7.1.6 CERTIFICAT QUALIFIE DE CACHET ELECTRONQUE (QCP-L)

7.1.6.1 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 création du certificat
Signature	Sha256WithRSAEncryption
Issuer	• CN=NETHEOS Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Subject	• C=<Pays d'enregistrement de l'autorité de certification> • O=<Organisation de la personne morale représentée par le cachet> • OU=ServerSeal • OI=<Identifiant d'organisation de la personne morale représentée par le cachet> • CN=Nom du cachet • serialNumber=<date de la création du certificat>

Validity	• notBefore: Date de création – 1 minute • notAfter: notBefore + 2 ans
Subject Public Key Info	RSA 3072 bits RSA 4096 bits

7.1.6.2 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	digitalSignature, nonRepudiation
basicConstraints	2.5.29.19	Non	• CA: False • Maximum Path Length : absent
cRLDistributionPoints	2.5.29.31	Non	Full Name: • URI: http://crl.netheos.com/sca.crl
authorityInfoAccess	1.3.6.1.5.5.7.1.1	Non	CA Issuers - URI: http://aia.netheos.com/aia/sca.crt
extendedKeyUsage	2.5.29.37	Non	
certificatePolicies		Non	policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.4.11 (Certificat de cachet de niveau QCP-l - processus d'identification en face à face physique) policyIdentifier = 1.3.6.1.4.1.55020.1.1.2.1 policyQualifiers = https://www.netheos.com/politique-denregistrement-politiques-de-certification

QCstatement	non	QCCompliance QcEuPDS https://ac.netheos.com/publications/pds.pdf QcType eSeal

7.2 LISTE DE CERTIFICATS REVOQUES

7.2.1 LCR

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 Swan CA • orgID=VATFR-78453023681 • O=NETHEOS • C=FR
Validity	7 jours
Revoked Certificates	• Serial Number • 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

7.2.1.3 OPTIONS

L'option "**Keep expired certificates on CRL**" est cochée.

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 biannuels minimum, diligentés par le responsable de la sécurité du système d'information ou son délégué ;
- Audits de certification biannuels, l'année suivante de l'audit interne ;
- 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 ou externes à la société NAMIRIAL, 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'auditeurs 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 et des certificats finaux ;
- Les données d'activation associées aux clés privées d'AC et aux certificats finaux ;
- Tous les secrets de l'IGC ;
- Les journaux d'événements des composantes de l'IGC ;
- Les formulaires de demande de génération et de révocation ;
- 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 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 au signataire 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 signataires 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 au signataire avant la signature des Documents Métier ;
- Protéger les données d'activation ;
- À collecter les données et pièces justificatives permettant de valide l'identité du signataire ;
- 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 signataires ;
- 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 NETHEOS pour les certificats de cachets. A ce titre elle s'engage à :

- Vérifier le contenu de la demande de certificat avant sa production ;
- Protéger les clés privées des certificats de cachets de manière à garantir que seul le Client en a le contrôle ;
- Traiter au plus tôt toute demande de révocation d'un certificat d'AC.

9.6.3 OBLIGATIONS DE L'AUTORITE D'ENREGISTREMENT DELEGUEE

L'AED a une obligation contractuelle avec NETHEOS de respecter les éléments ci-après :

- Identifier formellement les opérateurs d'enregistrement dans son organisation ;
- Réaliser les processus d'enregistrement conformément à ce qui est établit contractuellement ;
- Utiliser les interfaces mises à disposition par NETHEOS pour réaliser les opérations de vérification d'identité ;
- Accepter une clause d'audit permettant aux équipes NETHEOS ou à toute entité nommée par NETHEOS d'intervenir pour contrôler que les pratiques du Client sont en adéquation avec les attentes contractuelles.

9.6.4 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).

9.6.5 OBLIGATIONS DES RESPONSABLES DE CERTIFICAT DE CACHET

Les responsables de certificats de cachet doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- D'activer le certificat de cachet qui sera émis par NETHEOS ;
- De respecter les exigences qui lui incombent au titre de cette PC.

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+, et ETSI 319411-2 pour le niveau QCP-l, 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.