Netheos

Accélérez votre confiance digitale

AC NETHEOS

Conditions Générales d'Utilisation

NETHEOS Swan CA

Version	Date	Description	Auteurs	Société
1.0	29/05/2020	Correction définition	D.E	Netheos
1.1	14/09/2020	Correction O.I.D cachet NCP+	D.E	Netheos
1.2	22/09/2020	Corrections suite à l'audit	D.E	Netheos
1.3	19/11/2021	Correction mineure suite à audit interne	L.J	Netheos
1.4	04/10/2022	Mise à jour de la procédure de révocation	D.E	Netheos

Etat du document - Classification	Référence
Finalisé – C1	OID : 1.3.6.1.4.1.55020.1.1.2.3

1 INTRODUCTION

1.1 PRÉSENTATION GÉNÉRALE

NETHEOS opère une application de type SaaS délivrant un service de KYC (Know Your Customer) à leurs clients. Cette application est également évoquée sous le terme Service dans le cadre de ce document.

Souhaitant étendre son catalogue de produits, NETHEOS met en place une solution de signature électronique visant la conformité ETSI EN 319411-1 pour le niveau LCP ou NCP+ suivant le processus de délivrance. Le déploiement de cette solution nécessite la mise en œuvre d'une chaine de confiance permettant :

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

Ce document, appelé Conditions Générales d'Utilisation (CGU), reprend en synthèse les exigences décrites dans la Politique de Certification (PC) associée que doit faire respecter 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 ».

Les présentes CGU couvrent le déploiement des certificats finaux identifiés de la manière suivante :

- Certificat de signature de niveau LCP : 1.3.6.1.4.1.55020.1.1.2.4.5
- Certificat de signature de niveau NCP+ : 1.3.6.1.4.1.55020.1.1.2.4.1
- Certificat de cachet de niveau NCP+ : 1.3.6.1.4.1.55020.1.1.2.4.3

1.2 IDENTIFICATION DU DOCUMENT

Les présentes CGU sont identifiées par le numéro d'OID suivant : 1.3.6.1.4.1.55020.1.1.2.3

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

- .3 : CGU

1.3 DÉFINITIONS ET ACRONYMES

Les acronymes utilisés sont les suivants :

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

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.
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 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.
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 CONDITIONS GENERALES D'UTILISATION

2.1 POINT DE CONTACT

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

M. David EMO

Poste : Directeur technique

Adresse : NETHEOS, Les Centuries I, 93 place Pierre Duhem, 34000 Montpellier

Email : hello@netheos.com

Téléphone : (+33) 9 72 34 11 80

2.2 TYPES DE CERTIFICATS, PROCEDURES DE VALIDATION ET RESTRICTIONS D'USAGE

DOMAINES D'UTILISATION APPLICABLES

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.

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.

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

Le keyUsage est positionné à digitalSignature.

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.

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.

Le keyUsage est positionné à digitalSignature.

DOMAINES D'UTILISATION INTERDITS

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

NOMMAGE

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).

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 ».

ANONYMISATION OU PSEUDONYMISATION DES PORTEURS

Les certificats ne peuvent en aucun cas être anonymes.

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

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.

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. L'AC s'assure au moment de la validation de la demande que le certificat est unique pour l'identifiant d'entreprise concerné.

VALIDATION INITIALE DE L'IDENTITE

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.

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.

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).

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.

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.

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.

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 (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 (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 d'évaluation ;
- 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.

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.

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…).

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.

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

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.

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.

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.

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.

DEMANDE DE CERTIFICAT

ORIGINE D'UNE DEMANDE DE CERTIFICAT

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

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.

TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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 0. 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

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.

DELIVRANCE DU CERTIFICAT

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. Cela est applicable pour l'ensemble des certificats émis par l'AC.

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
    - Générer la demande technique de certificat correspondant aux informations fournies par le RC
    - Faire signer la demande technique de certificat par le certificat de l'AC
    - Déclencher la génération d'un code d'activation qui sera transmis par téléphone au RC
- 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.

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.

ACCEPTATION DU CERTIFICAT

DEMARCHE D'ACCEPTATION DU CERTIFICAT

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

L'acceptation du certificat vaut pour confirmation que les informations présentes à l'intérieur de celui-ci sont correctes.

PUBLICATION DU CERTIFICAT

Les certificats finaux ne sont pas publiés.

REVOCATION ET SUSPENSION DES CERTIFICATS

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 des CGUs;
- 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.

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.

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
- Notification par email du porteur de certificat du traitement de sa demande de révocation

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
- Notification via le ticket support du RC du traitement de sa demande de révocation

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.

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.

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.

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.

2.3 LIMITES D'ENGAGEMENT

USAGE DE LA CLE PUBLIQUE ET DU CERTIFICAT

CERTIFICATS DES AC OPERATIONNELLES

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

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

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.

ARCHIVAGE

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

LIMITE DE RESPONSABILITE

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 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.

2.4 OBLIGATIONS

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.

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.

OBLIGATIONS DES CLIENTS

Le Client en tant qu'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.

OBLIGATIONS DU SIGNATAIRE

En acceptant d'utiliser ce service, le Signataire accepte de respecter des modalités les présentes CGU et de :

- Fournir au Client et à l'AC des informations exactes et authentiques ;
- Protéger la sécurité et la confidentialité du code temporaire transmis par l'AC et reçu par SMS utilisé pour signer le(s) document(s). Ce code doit être détruit par l'Utilisateur après avoir procédé à la signature électronique ;
- Vérifier le contenu du Certificat et alerter le Client ou l'AC si le Certificat n'est pas correctement rempli ;
- Vérifier l'authenticité et l'exactitude des informations à indiquer dans le Certificat et à utiliser pour recevoir le code temporaire, telles qu'elles sont présentées lors du parcours client ;
- Demander dans les meilleurs délais la révocation du Certificat au Client ou à l'AC, si besoin est ;
- Aviser dans les plus brefs délais, le Client de tout changement concernant les moyens d'authentification utilisés par le Client et l'AC (numéro de téléphone et adresse de courrier électronique)

2.5 STATUTS DES 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.

FREQUENCE D'ETABLISSEMENT DES LCR

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

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.

LIMITES DE GARANTIE

Sans objet.

2.6 DOCUMENTS APPLICABLES

Les informations publiées sont les suivantes :

- La 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 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/

2.7 POLITIQUE SUR LES DONNÉES PERSONNELLES

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

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

En acceptant ces CGU, le signataire consent au traitement et à la conservation des ses données personnelles.

2.8 POLITIQUE DE REMBOURSEMENT

Sans objet.

2.9 LOI APPLICABLE

En cas de contestation sur l'interprétation ou l'exécution de l'une quelconque des dispositions des CGUs 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.

2.10 CERTIFICATIONS ET CONDITIONS D'AUDIT

MATERIELS 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.

CERTIFICATION DU SERVICE

Des audits externes sont 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.

Les cibles de certification ETSI sont les suivantes : ETSI EN 319411-1 pour le niveau LCP ou NCP+.

Signé par Netheos le 05/10/2022 à 12:33:02 CEST