Netheos

Accélérez votre confiance digitale

Service PVID Netheos

Politique de Vérification d'identité à Distance

Version	Date	Description	Auteurs	Société
1.0	29/10/2021	Version finalisée	Netheos	Netheos
1 1	03/11/2021	Version relue	D.Emo	Netheos
1.2	28/04/2022	Corrections diverses	D.Emo	Netheos
1.3	17/05/2022	Mise à jour suite à audit interne	D.Emo	Netheos
1.4	20/06/2022	Corrections suite à l'audit	D.Emo	Netheos
1.5	18/08/2023	Ajout des documents supportés	D.Emo	Netheos

Etat du document - Classification	Référence
Finalisé - C1	OID : 1.3.6.1.4.1.55020.1.1.30.1.5

1 INTRODUCTION 7
1.1 PRESENTATION GENERALE 7
1.2 IDENTIFICATION DU SERVICE ET DU DOCUMENT 7
1.3 ENTITES INTERVENANT DANS LE SERVICES 7
1.3.1 Fournisseur du service 7
1.3.2 service métier 8
1.3.3 Clients 8
1.3.4 Utilisateur du service 8
1.3.5 Autres participants 8
1.4 DOMAINES D'UTILISATION DU SERVICE 8
1.5 GESTION DE LA PRESENTE POLITIQUE 9
1.5.1 Entité gérant la Politique 9
1.5.2 Point de contact 9
1.5.3 Documentation mise à disposition 9
1.5.4 Entité déterminant la conformité d'une déclaration des pratique avec la présente politique 10
1.5.5 Procédures d'approbation de la conformité 10
1.6 DEFINITION ET ACRONYMES 10
1.6.1 Abréviations 10
1.6.2 Définitions 11
2 DESCRIPTION DU SERVICE DE VERIFICATION A DISTANCE 11
2.1 PRESENTATION GENERALE DU SERVICE 11
2.2 ACQUISITION DES DONNEES D'IDENTIFICATION 12
2.2.1 Terminal d'acquisition des données 12
2.2.2 Interface utilisateur du service 13
2.2.3 Parcours d'acquisition des données d'identification 13
2.3 VERIFICATION DES DONNEES D'IDENTIFICATION 13
2.3.1 Principe de la vérification 13
2.3.2 Vérification de l'authenticité et de la validité du titre d'identité 14
2.3.3 Vérifications du visage de l'utilisateur et détection du vivant 15
2.3.4 Titre d'identité acceptés 15
2.4 CONSTITUTION DU DOSSIER DE PREUVE 16
2.4.1 Contenu du dossier de preuve 16
2.4.2 Conservation du dossier de preuve 17
2.4.3 Droits d'accès et modification du dossier de preuve 18

2.5 TRANSMISSION DU RESULTAT AU SERVICE METIER. 18
2.5.1 Constitution du résultat 18
2.5.2 Transmission du résultat 19
2.6 GESTION DE LA FRAUDE 19
2.7 GESTION DES RECLAMATIONS 20
2.8 GESTION DES DONNEES A CARACTERE PERSONNEL 20
2.8.1 Alternative à la biométrie 20
2.8.2 Minimisation et liste des données traitées 21
2.8.3 Traitement biométrique 21
2.8.4 Modalité de traitement des données personnelles 21
3 GESTION DU RISQUE 24
3.1 APPRECIATION ET TRAITEMENT DES RISQUES 24
3.1.1 Analyse de risque 24
3.1.2 Traitement du risque 25
3.2 PLAN DE TEST DE LA CAPACITE EFFECTIVE DU SERVICE A DETECTER DES TENTATIVES D'USURPATION D'IDENTITE 25
4 PROTECTION DE L'INFORMATION 25
4.1 TERMINAL 26
4.2 POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION 26
4.3 HOMOLOGATION 26
4.4 LOCALISATION DES DONNEES. 26
4.5 NIVEAU DE SECURITE 26
4.6 CONTROLE 26
4.7 SECURITE PHYSIQUE 27
4.8 JOURNALISATION 27
4.8.1 Type d'événement à enregistrer 28
4.8.2 Fréquence de traitement des journaux d'événements 28
4.8.3 Période de conservation des journaux d'événements 28
4.8.4 Protection des journaux d'événements 28
4.8.5 Procédure de sauvegarde des journaux d'événements 28
4.8.6 Système de collecte des journaux d'événements 28
4.9 SAUVEGARDES 29
4.10 CLOISONNEMENT 29
4.11 ADMINISTRATION ET EXPLOITATION DU SERVICE 29
4.12 INTERCONNEXIONS DU SYSTEME D'INFORMATION DU SERVICE 30

4.13 ACCES DISTANT 30
4.14 DEVELOPPEMENT ET SECURITE DES LOGICELS 30
4.15 GESTION DES INCIDENTS 31
5 ORGANISATION DU PRESTATAIRE ET GOUVERNANCE 31
5.1 RECRUTEMENT 31
5.1.1 Procédures de vérification des antécédents 31
5.1.2 Exigences en matière de formation initiale 31
5.2 CHARTE D'ETHIQUE 32
5.3 ORGANISATION ET GESTION DES COMPETENCES 32
5.3.1 Nombre de personnes requises par tâche 32
5.3.2 Documentation fournie au personnel 32
5.3.3 Formation continue 33
5.3.4 Plan de controle 33
5.3.5 Bulletin opérationnel 33
5.3.6 Relation avec les services de l'état 33
5.4 ROLES DE CONFIANCE 34
5.4.1 Administrateur 34
5.4.2 Opérateur 34
5.4.3 Référent Fraude Biométrie 35
5.4.4 Référent Fraude Titre 36
5.4.5 Officier de sécurité 36
6 QUALITE ET NIVEAU DE SERVICE 37
6.1 QUALITE DU SERVICE 37
6.2 CONVENTION DE SERVICE 37
7 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS 37
7.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS 38
7.2 IDENTITES ET QUALIFICATION DES EVALUATEURS 38
7.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES 38
7.4 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS 38
7.5 COMMUNICATION DES RESULTATS 39
8 AUTRES PROBLEMATIQUES METIERS ET LEGALES 39
8.1 TARIF 39
8.2 RESPONSABILITE FINANCIERE 39
8.2.1 Couverture par les assurances 39

8.2.2 Autres ressources 39
8.2.3 Couverture et garantie concernant les entités utilisatrices 39
8.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES 39
8.3.1 Périmètre des informations confidentielles 39
8.3.2 Informations hors du périmètre des informations confidentielles 40
8.3.3 Responsabilités en termes de protection des informations confidentielles 40
8.4 PROTECTION DES DONNEES PERSONNELLES 40
8.4.1 Politique de protection des données personnelles 40
8.4.2 Informations à caractère personnel 40
8.4.3 Informations à caractère non personnel 40
8.4.4 Responsabilité en termes de protection des données personnelles 40
8.4.5 Notification et consentement d'utilisation des données personnelles 40
8.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives 40
8.4.7 Autres circonstances de divulgation d'informations personnelles 41
8.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE 41
8.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES 41
8.6.1 Obligations du service PVID 41
8.6.2 Obligations des utilisateurs du service 41
8.7 LIMITE DE GARANTIE 42
8.8 LIMITE DE RESPONSABILITE 42
8.9 INDEMNITES 42
8.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PRESENTE POLITIQUE 42
8.10.1 Durée de validité 42
8.10.2 Fin anticipée de validité 42
8.10.3 Effets de la fin de validité et clauses restant applicables 42
8.10.4 Notifications individuelles et communications entre les participants 43
8.11 AMENDEMENTS A LA POLITIQUE 43
8.11.1 Procédures d'amendements 43
8.11.2 Mécanisme et période d'information sur les amendements 43
8.11.3 Circonstances selon lesquelles l'OID doit être changé 43
8.12 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS 43
8.13 JURIDICTIONS COMPETENTES 43
8.14 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS 43
8.15 DISPOSITION DIVERSES 44

8.15.1 Accord global 44
8.15.2 Transfert d'activités 44
8.15.3 Conséquences d'une clause non valide 44
8.15.4 Application et renonciation 44
8.16 FORCE MAJEURE 44
8.17 AUTRES DISPOSITIONS 44

1 INTRODUCTION

1.1 PRÉSENTATION GÉNÉRALE

NETHEOS opère une application de type SaaS délivrant un service de souscription numérique à ses clients. Cette application est également évoquée sous le terme Service dans le cadre de ce document.
Afin de compléter son offre, NETHEOS met en place une solution de vérification d'identité à distance visant la conformité au cahier des charges PVID de l'ANSSI pour le niveau Substantiel. 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.) ;
- L'identification fiable et à distance des utilisateurs.

Ce document, appelé Politique de Vérification d'Identité à Distance (PoVID), décrit les exigences à respecter par le service de vérification d'identité à distance NETHEOS.

Cette version du document est applicable à partir du 18/08/2023.

1.2 IDENTIFICATION DU SERVICE ET DU DOCUMENT

Le service de vérification d'identité à distance est identifié par le numéro d'OID suivant : 1.3.6.1.4.1.55020.1.1.30

La présente Politique est identifiée par le numéro d'OID suivant : 1.3.6.1.4.1.55020.1.1.30.1.X (X étant son numéro de version).

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
      - .30 : Service PVID
        - .1 : Politique de Vérification d'identité à Distance

1.3 ENTITES INTERVENANT DANS LE SERVICES

Nous présentons dans cette section les différentes entités liées au service.

1.3.1 FOURNISSEUR DU SERVICE

Netheos est la personne morale identifiée comme le fournisseur du service de vérification d'identité à distance.

Le fournisseur du service est en charge de la réalisation des quatre étapes suivantes :

- L'acquisition des données d'identification ;
- La vérification des données d'identification ;
- La constitution du dossier de preuve ;
- La transmission des résultats au service métier.

Cette entité est nommée « Prestataire » ou « PVID » dans le référentiel d'exigences de l'ANSSI ([ANSSI_PVID]).

1.3.2 SERVICE METIER

Netheos opère le service de vérification à distance pour son propre compte, afin d'élargir les fonctionnalités de sa plate-forme de contractualisation en ligne. En ce sens, cette plate-forme est actuellement le seul service métier autorisé à se connecter au service PVID. En ce sens, Netheos est donc le commanditaire au sens du référentiel d'exigences de l'ANSSI (ANSSI_PVID).

Les futures versions de la présente politique pourront envisager d'ouvrir le service PVID à d'autres commanditaires, et donc d'autres services métiers.

1.3.3 CLIENTS

Les clients de Netheos sont les personnes morales ayant contractualisé avec Netheos afin d'utiliser la plate-forme de contractualisation en ligne de Netheos dans le cadre d'une entrée en relation à distance. Le parcours de contractualisation pourra, suivant les exigences du client et/ou les choix de l'utilisateur du service (voir plus bas), inclure un parcours faisant intervenir le service de vérification d'identité à distance.

N'opérant pas directement service métier en interaction avec le service PVID, le client ne répond pas strictement à la notion de « commanditaire », tel que défini dans le référentiel d'exigences de l'ANSSI (ANSSI_PVID). Cependant, certaines exigences du référentiel, de part un rôle proche du commanditaire, leur sont applicables.

1.3.4 UTILISATEUR DU SERVICE

Les utilisateurs du service de vérification d'identité à distance sont des personnes physiques accédant au service afin que leur identité soit vérifiée pour le compte du client défini ci-dessus, afin de contractualiser avec ce dernier.

La dénomination « Utilisateur » est aussi employée dans le référentiel d'exigences de l'ANSSI ([ANSSI_PVID]).

1.3.5 AUTRES PARTICIPANTS

Sans objet.

1.4 DOMAINES D'UTILISATION DU SERVICE

Le service est destiné à la vérification d'identité à distance dans le cadre :

- De l'entrée en relation d'affaire à distance conformément aux dispositions prévues par le décret n° 2020-118 du 12 février 2020 ;
- D'un service de confiance régi par le règlement eIDAS et nécessitant la vérification d'identité d'une personne physique pour la délivrance d'un certificat électronique.

Des clients évoluant dans d'autres domaines peuvent souscrire au service dans la mesure où la règlementation applicable au client pour ce cas d'usage ne l'interdit pas. Le client prend l'entière responsabilité de la décision de recourir au service de vérification d'identité à distance objet de la présente politique.

1.5 GESTION DE LA PRESENTE POLITIQUE

1.5.1 ENTITE GERANT LA POLITIQUE

La Politique est gérée par le Comité de Suivi des Services de Confiance (C2SSC).

1.5.2 POINT DE CONTACT

Toute information concernant la présente Politique ou la gestion du service peut être demandée via le point de contact suivant :

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

1.5.3 DOCUMENTATION MISE A DISPOSITION

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

- La présente Politique ;
- Les conditions générales du service associée ;

La présente Politique 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 :

- https://www.netheos.com/pvid/230818_C1_DEM_v1.5_politique_de_verification_d_identite_a_distance

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 du fournisseur de service. 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.

Netheos maintient un ensemble de documents destinés à garantir la fiabilité du service et le respect de ses engagements en tant que fournisseur du service, en particulier la Déclaration des pratiques de vérification d'identité à distance (DPVID) : Ce document décrit un ensemble de pratiques (organisation, procédures opérationnelles, moyens techniques et humains, etc.) mises en œuvre dans le cadre de la fourniture du service, en conformité avec la présente politique de vérification d'identité à distance. La déclaration fait référence, par son OID, à la politique de vérification d'identité à distance à laquelle elle se rapporte. Le document est confidentiel et n'est mis à disposition que des seules personnes ayant le besoin d'en connaître. Le contenu de ce document est conforme aux exigences issues du référentiel émis par l'ANSSI ([ANSSI_PVID]).

1.5.4 ENTITE DETERMINANT LA CONFORMITE D'UNE DECLARATION DES PRATIQUE AVEC LA PRESENTE POLITIQUE

La conformité de la DPVID à la présente politique est validée par le C2SSC.

1.5.5 PROCEDURES D'APPROBATION DE LA CONFORMITE

Netheos s'assure de la cohérence des documents publiés avec les engagements, les exigences et les pratiques en vigueur sur le service. La présente politique entre en vigueur à compter de sa mise à disposition sur le site de publication et est valide jusqu'à la prise d'effet d'une nouvelle version.

Netheos contrôle que tout projet de modification de la présente politique reste conforme aux exigences réglementaires et normatives applicables, et en particulier :

- Toute mise à jour concernant les sujets relatifs à la biométrie nécessite une validation formelle du référent fraude Biométrie ;
- Toute mise à jour concernant les sujets relatifs aux titres d'identité nécessite une validation formelle du référent fraude Titre d'identité.

Toute évolution majeure de la politique du service implique son identification par un OID distinct des précédentes versions.

En cas d'évolution du service, Netheos s'engage à publier la documentation correspondante avant la mise en service de ces évolutions et s'efforce de prévenir les clients et les utilisateurs afin qu'ils puissent adopter les dispositions qui s'imposent.

L'approbation de la conformité est prononcée par le responsable du C2SSC 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 Politique sont les suivants :

1.6.1 ABREVIATIONS

C2SSC Comité de Suivi des services de confiance

CEN Comité Européen de Normalisation

DPVID Déclaration des Pratiques de vérification d'identité à distance

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)

OID Object Identifier (identifiant universel d'un objet)

PSCo Prestataire de Services de Confiance

RSA Rivest Shamir Adeleman

SSI Sécurité des Systèmes d'Information

1.6.2 DEFINITIONS

Authentification	Processus permettant de vérifier l'identité déclarée d'une personne ou de toute autre entité, ou de garantir l'origine de données reçues.
Bi clé	Une bi clé est un couple composé d'une clé privée (devant être tenue secrète) et d'une clé publique, nécessaire à la mise en œuvre de techniques cryptologiques basées sur des algorithmes asymétriques.
HSM	Boîtier cryptographique matériel dans lequel sont stockées les clés privées utilisées pour le déchiffrement.
Object Identifier	Identificateur numérique unique enregistré conformément à la norme d'enregistrement ISO (ISO/IEC 9834-1:2012) pour désigner un objet ou une classe d'objets spécifiques.
Produit de sécurité	Dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.
Système d'information	Tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci.

2 DESCRIPTION DU SERVICE DE VERIFICATION A DISTANCE

2.1 PRÉSENTATION GÉNÉRALE DU SERVICE

La vérification d'identité à distance se décompose en quatre étapes successives :

- Acquisition des données d'identification (voir au §2.2) :

L'utilisateur réalise un parcours sur mobile durant lequel il doit présenter son visage et un titre d'identité valide pendant la phase d'acquisition des données. Des données complémentaires peuvent être fournis par l'utilisateur au service de vérification d'identité à distance à la discrétion du commanditaire. Celles-ci ne rentrent pas en compte dans l'évaluation du verdict retourné par le service de vérification d'identité à distance.

- Vérification des données d'identification (voir au §2.3) :

Le service de vérification d'identité à distance est de type « asynchrone » : les tâches de vérification des données d'identification sont réalisées postérieurement à l'acquisition des données d'identification.

La vérification des données d'identification ne peut aboutir avec succès qu'après intervention d'un opérateur (personne physique) du service de vérification d'identité à distance. Ainsi, le service est dit « hybride » au sens du référentiel d'exigences de l'ANSSI ([ANSSI_PVID]).

- Constitution du dossier de preuve (voir au §2.4) :

Le dossier de preuve est généré quel que soit le résultat de la vérification d'identité, et est conservé par Netheos pour servir notamment en cas de litige.

- Transmission des résultats au service métier (voir au §2.5).

Le résultat est transmis au service métier pour lequel l'utilisateur s'est identifié une fois le dossier de preuve constitué et enregistré. Le résultat intègre le verdict de la vérification d'identité ainsi que des attributs d'identité de l'utilisateur. Les attributs peuvent être utilisés par le service métier pour :

- S'assurer de la cohérence entre les données vérifiées par le service PVID et les données de contractualisation
- Permettre d'émission d'un certificat de signature électronique, éventuellement qualifié.

Netheos, en tant que fournisseur du service, garantit de plus :

- La gestion de la fraude (voir au §2.6);
- La gestion des recours et réclamations des utilisateurs (voir au §2.7);
- L'encadrement de l'utilisation du service par les utilisateurs (voir au §2.8);
- La relation contractuelle et opérationnelle avec les clients (voir au §2.9) ;
- La protection des données à caractère personnel (voir au §2.10).

2.2 ACQUISITION DES DONNÉES D'IDENTIFICATION

Cette étape consiste à acquérir les données d'identification relatives à l'utilisateur, à savoir une vidéo montrant le titre d'identité de l'utilisateur et une vidéo montrant son visage.

2.2.1 TERMINAL D'ACQUISITION DES DONNEES

Un utilisateur accède au service de vérification d'identité à distance depuis son propre terminal mobile :

- via une application mobile mise à disposition par le client du service (pour ses propres besoins métier) et intégrant une interface vers le service métier intégrant le parcours de vérification à distance de Netheos ou intégrant directement le parcours de vérification à distance de Netheos ;

- via un portail web mis à disposition par le client du service (pour ses propres besoins métier) et intégrant une interface vers le service métier intégrant le parcours de vérification à distance de Netheos ou intégrant directement le parcours de vérification à distance de Netheos ;

Le service ne nécessite pas l'installation d'une application spécifique sur le terminal de l'utilisateur. Lorsqu'une application mobile est mise à disposition par le client, ce dernier est responsable de l'intégrité de cette application et de la sécurité des données qu'elle recueille et transmet.

Le terminal doit être équipé d'un dispositif de capture vidéo (avant et arrière) capable de produire une vidéo de résolution minimale 720p (1280×720) à 25 images par seconde. Il doit être également équipé d'un microphone.

2.2.2 INTERFACE UTILISATEUR DU SERVICE

L'interface présentée à l'utilisateur a comme unique objectif l'acquisition de séquences vidéo qui seront soumises au service pour la vérification de l'identité. Cette interface guide l'utilisateur dans le processus d'acquisition de façon automatisée, sans intervention d'un opérateur du service. Elle est disponible a minima en Français[1].

2.2.3 PARCOURS D'ACQUISITION DES DONNEES D'IDENTIFICATION

L'interface du service affiche à l'utilisateur les consignes liées aux phases successives de l'acquisition des données d'identification :

- Présentation du processus ;
- Indication que le processus d'identification se déroule en langue française ;
- Présentation des
  - Conditions Générales d'Utilisation pour acceptation ;
  - Demande de consentement spécifique aux traitements des données biométrique ;
- Présentation de la liste des documents d'identité acceptés et choix de l'utilisateur ;
- Capture de la pièce d'identité de l'utilisateur avec un challenge anti-rejeu
- Capture du visage de l'utilisateur avec un challenge anti-rejeu

Conformément à l'exigence de la CNIL, la solution faisant appel à la biométrie, une méthode alternative est systématiquement proposée en amont du parcours.

Il est demandé à l'utilisateur :

- De s'assurer que les conditions de lumières sont suffisantes
- De ne pas porter d'éléments gênant l'identification vidéo en particulier : chapeau, masque sur la base du visage, lunette de soleil.

2.3 VÉRIFICATION DES DONNÉES D'IDENTIFICATION

Sur la base des données d'identification acquises lors de l'étape précédente, cette étape consiste à vérifier, par des traitements automatisés puis par une vérification d'un opérateur humain, que :

- Le titre d'identité présenté par l'utilisateur est authentique ;
- L'utilisateur est le détenteur légitime du titre d'identité.

2.3.1 PRINCIPE DE LA VERIFICATION

[1] D'autres langues pourront être ajoutées à la demande des clients de Netheos.

La vérification des données d'identification suit le processus suivant :

- Les vidéos acquises à l'étape précédente sont analysées par un traitement automatisé. Cette analyse :
  - Vérifie que la résolution de la vidéo acquise à l'étape précédente possède bien une résolution minimale de 720p (1280 × 720) à 25 images par seconde ;
  - Extrait des attributs d'identité de l'utilisateur ;
  - Génère des constats intermédiaires concernant à la fois le titre d'identité, le visage de l'utilisateur et le caractère « vivant » de ce dernier ;
- Les vidéos acquises à l'étape précédente, leurs extraits, ainsi que les attributs et constats générés par les traitements automatisés, sont vérifiés par un opérateur humain du service
  - Vérification de l'exactitude des attributs d'identité de l'utilisateur extrait de la pièce ;
  - Vérification de l'authenticité du titre d'identité, de la correspondance du visage de l'utilisateur avec la photo du titre d'identité et du caractère « vivant » de l'utilisateur ;
- L'opérateur humain détermine le verdict final de la vérification d'identité.
  - En cas d'incohérence entre l'avis de l'opérateur humain et l'avis de la machine une alerte est réalisée
  - En cas de doute de l'opérateur humain, une escalade au référent fraude est réalisée en fin de parcours de vérification.

Les seuls titres d'identité acceptés par le service de vérification sont présentés au §2.3.4. Lorsque l'utilisateur présente un autre type de titre, le verdit du service est toujours « échec ».

Les titres d'identité présentant une altération physique (titre d'identité déchiré ou écorné, etc.) font systématiquement l'objet d'un verdict « échec ».

Si les vidéos acquises ne satisfont pas aux critères de résolution minimale ou bien de nombre d'images par seconde minimal alors le verdit du service est toujours « échec ».

Le verdict est « succès » si le service de vérification d'identité à distance conclut que le titre d'identité présenté par l'utilisateur est authentique d'une part et que l'utilisateur est le légitime détenteur du titre d'identité d'autre part, sinon le verdict est « échec ».

Les contrôles réalisés durant la phase d'acquisition de la vidéo visent uniquement à assurer une qualité suffisante pour la vidéo enregistrée. Aucun contrôle réalisé sur le terminal de l'utilisateur ne peut contribuer au verdict « succès » de la vérification d'identité à distance.

Des mesures de sécurité, confidentielles et seulement documentées dans la déclaration des pratiques de vérification d'identité à distance, sont mises en œuvre pour la détection des tentatives de fraude, la protection de certains types d'utilisateurs ou la détection des attaques récurrentes.

2.3.2 VERIFICATION DE L'AUTHENTICITE ET DE LA VALIDITE DU TITRE D'IDENTITE

Il est vérifié les points suivants :

- Le date d'expiration du titre d'identité n'est pas dépassée ;
- Le titre apparaît authentique. En particulier, des éléments de sécurité associés au titre d'identité et décrits sur le registre public en ligne des documents authentiques d'identité et de voyage (PRADO) sont vérifiés.

Le détail des vérifications réalisées et des moyens mis en œuvre est confidentiel et est décrit dans la déclaration des pratiques.

Pour l'ensemble des titres acceptés et listés au §2.3.4, il n'existe pas, à la date de publication de la présente politique, de service de vérification de la validité de ces titres d'identité mis à disposition de l'Etat en charge de leur émission. Dès lors que l'État responsable de l'émission d'un titre d'identité mettrait à disposition de Netheos un service de vérification de validité :

- Le service de vérification d'identité à distance solliciterait systématiquement ce service ;
- Le verdict de la vérification d'identité à distance est systématiquement « échec » si le résultat de cet appel indique que le titre d'identité est invalide.

Les informations suivantes sont extraites du titre d'identité présenté :

- Les noms et prénoms du porteur ;
- Le sexe du porteur ;
- La date et le lieu de naissance de naissance du porteur ;
- Le numéro unique du titre d'identité ;
- La date de délivrance du titre d'identité ;
- La date d'expiration du titre d'identité.

Lorsque l'opérateur humain sélectionne un verdict différent de celui proposé par le traitement automatisé, un enregistrement est effectué et une alerte est envoyée au référent fraude Titre d'identité si l'opérateur donne un verdict « succès » alors que le traitement automatisé proposait « échec ».

2.3.3 VERIFICATIONS DU VISAGE DE L'UTILISATEUR ET DETECTION DU VIVANT

Les vérifications effectuées sur le visage de l'utilisateur ont pour objectifs de :

- Vérifier la similitude du visage extrait de la vidéo de l'utilisateur avec la photographie extrait de la vidéo du titre d'identité ;
- Vérifier le caractère « vivant » de l'utilisateur représenté dans la vidéo.

Chacune de ces vérifications donne lieu à un constat intermédiaire. Les vérifications réalisées pour la détection du vivant et la correspondance des visages sont confidentielles et détaillées uniquement dans la déclaration des pratiques de vérification associée à la présente politique.

Lorsque l'opérateur humain sélectionne un verdict différent de celui proposé par le traitement automatisé, un enregistrement est effectué et une alerte est envoyée au référent fraude Biométrie si l'opérateur donne un verdict « succès » alors que le traitement automatisé proposait « échec ». La procédure d'escalade associée est confidentielle et est détaillée dans la déclaration des pratiques.

2.3.4 TITRE D'IDENTITE ACCEPTES

Les titres d'identité acceptés par le service sont listés dans le tableau suivant :

Pays émetteur	Type de titre	**Première émission**	**Référence PRADO**
France	Carte nationale d'identité	15/03/2021	FRA-BO-03001
France	Carte nationale d'identité	01/10/1994	FRA-BO-02002
France	Passeport	13/04/2019	FRA-AO-03004
France	Passeport	02/04/2013	FRA-AO-03003
France	Passeport	28/10/2008	FRA-AO-03002
France	Titre de séjour	20/06/2011	FRA-HO-09001
France	Titre de séjour	10/08/2020	FRA-HO-12001

Les prochaines versions de la présente politique pourront étendre la liste des titres acceptés.

A chacun de ces titres d'identité est associé, au sein du personnel du service, au moins un référent fraude Titre d'identité compétent.

La politique de vérification d'identité à distance doit identifier les attributs du titre d'identité qui caractérisent l'unicité de l'identité d'une personne physique. Cette unicité s'appuie sur les attributs suivants :

- Nom et prénoms
- Date de naissance
- Commune de naissance.

2.4 CONSTITUTION DU DOSSIER DE PREUVE

Cette étape consiste à créer un dossier de preuve comprenant les données d'identification acquises, les constats intermédiaires issus des traitements automatisés et humains de la vérification des données d'identification ainsi que le résultat de la vérification d'identité transmis au service métier.

2.4.1 CONTENU DU DOSSIER DE PREUVE

Chaque vérification d'identité, quel que soit le verdict (« succès » ou « échec »), fait l'objet de la création d'un dossier de preuve. Ce dossier est constitué afin de pouvoir fournir toutes les informations nécessaires à la résolution des litiges.

Les éléments constitutifs du dossier de preuve sont :

- Les informations relatives aux données d'identification :
    - La date d'acquisition de la vidéo ;
    - La vidéo acquise auprès de l'utilisateur (cf. §2.2) ;
- La liste de l'ensemble des vérifications réalisées sur les données d'identification, et pour chaque vérification :

- La date de la vérification ;
- L'activité associée à la vérification, notamment :
    - Vérification de l'authenticité du titre d'identité ;
    - Détection du caractère « vivant » de l'utilisateur ;
    - Comparaison du visage de l'utilisateur ;
- La nature de la vérification : automatique ou manuelle ;
- Pour une vérification manuelle :
    - L'identité de l'opérateur ou du référent fraude qui a procédé à la vérification ;
    - Le pays depuis lequel l'opérateur ou le référent fraude a réalisé la vérification ;
- Pour une vérification automatique :
    - La version et la configuration le cas échéant des outils ayant réalisé la vérification
- Le constat intermédiaire rendu par les traitements automatisés, l'opérateur ou le référent fraude à la suite de la vérification ;
    - Les informations relatives aux verdicts de la vérification d'identité à distance
- Le verdict final : « succès » ou « échec » ;
- Les motifs rendus par l'opérateur en cas de verdict « échec » ;
- L'identité de l'opérateur qui a prononcé le verdict ;
- La date à laquelle le verdict a été prononcé par l'opérateur
- Le pays depuis lequel l'opérateur a prononcé le verdict
    - Les informations relatives à l'utilisateur :
- Nom ;
- Prénoms ;
- Date de naissance ;
- Lieu de naissance :
    - Les informations relatives au titre d'identité :
- Numéro unique du titre d'identité ;
- Date de délivrance du titre d'identité ;
- Date d'expiration du titre d'identité ;
    - Le résultat de la vérification d'identité à distance transmis au client.

Aucune des données contenues dans le dossier de preuve n'a pour finalité un traitement biométrique (voir §2.4.3).

2.4.2 CONSERVATION DU DOSSIER DE PREUVE

Le dossier de preuve est versé par le service de vérification d'identité à distance dans un espace d'archivage dédié au service, assurant l'intégrité, la confidentialité et la disponibilité des données.

La durée de conservation du dossier de preuve est de 7 ans après la date de vérification par le service pour :

- Être toujours disponible en cas de contentieux à propos d'une identification réalisée (que ce contentieux provienne du client ou de l'utilisateur) ;

- Satisfaire aux durées de conservation des éléments de preuve spécifiées dans les services de confiance ou les identités électroniques régis par le règlement eIDAS et reposant sur le service de vérification d'identité à distance ;

Les dossiers de preuves font l'objet d'une procédure de destruction à la fin de la période de conservation

Les dossiers de preuve sont chiffrés dès leur création à l'aide d'un mécanisme cryptographique reposant sur une bi-clé asymétrique. La clé de déchiffrement est mise en œuvre dans un équipement cryptographique sécurisé.

2.4.3 DROITS D'ACCES ET MODIFICATION DU DOSSIER DE PREUVE

La bi-clé de chiffrement est générée par le matériel cryptographique sécurisé dans le cadre d'une opération strictement contrôlée en présence de plusieurs personnels de confiance de Netheos. La clé privée de chiffrement n'est jamais extraite du matériel cryptographique sécurisé excepté pour la réalisation de copies de sauvegardes conservées dans des conditions de sécurité au moins équivalentes au stockage interne du matériel cryptographique sécurisé.

Un dossier de preuve archivé peut être consulté uniquement dans des circonstances exceptionnelles, telles qu'une réquisition judiciaire, une demande utilisateur, un contentieux ne pouvant être traité sans le dossier de preuve ou la recherche de fraudes par exemple.

L'utilisation de la clé de chiffrement est restreinte nécessite aux seules personnes ayant le besoin d'en connaitre parmi une liste de personnes prédéterminée et contrôlée par le responsable de la sécurité du service. La présence d'au moins deux personnes distinctes de confiance de Netheos est requise pour tout déchiffrement d'un dossier de preuve.

Les utilisateurs disposent d'un droit d'accès aux données à caractère personnel les concernant et notamment celles contenues dans le dossier de preuve. Toutefois les utilisateurs ne peuvent pas exercer de droit de rectification sur le contenu du dossier afin de conserver intactes les données acquises par le service et ne pas diminuer la force probante de ce dossier.

2.5 TRANSMISSION DU RESULTAT AU SERVICE METIER.

Cette étape consiste à transmettre au service métier de Netheos, et le cas échéant, dans le futur, à un service métier du client, le résultat comprenant le verdict (échec ou succès) de la vérification d'identité, le motif de l'échec le cas échéant, et les attributs d'identité relatifs à l'utilisateur et vérifiés par le service.

2.5.1 CONSTITUTION DU RESULTAT

Le résultat de la vérification d'identité à distance est transmis au service métier systématiquement, quel que soit le verdict (« succès » ou « échec »).

Le résultat de la vérification d'identité à distance est constitué des seules informations suivantes :

- Verdict (« succès » ou « échec ») de la vérification ;
- Cause de refus : Fraude, Qualité, Erreur humaine, Expiration ou autre ;
- Les contrôles de cohérence entre le document et les informations complémentaires d'identité de l'utilisateur ;

- Attributs d'identité relatifs à l'utilisateur :
  - Nom ;
  - Prénoms ;
  - Genre ;
  - Date de naissance ;
  - Lieu de naissance ;
  - Photo du visage extraite de la vidéo
  - Photo du titre d'identité
  - Informations du titre d'identité

Aucune autre information supplémentaire n'est ajoutée à ce résultat. En particulier :

- La vidéo du titre d'identité et du visage de l'utilisateur ne sont d'aucune manière, ni totalement ni partiellement, transmises au service métier. Par exception, une photo du visage de l'utilisateur et une photo du titre d'identité peuvent être extraites de la vidéo et intégrée au résultat de la vérification ;
- Le résultat ne contient aucun élément relatif aux constats issus des vérifications réalisées par le service autre que le verdict indiqué, et notamment aucun score calculé sur la base de ces vérifications ;
- Le service ne recueille et ne transmet aucune donnée complémentaire par rapport à la vidéo du visage et du titre d'identité.

2.5.2 TRANSMISSION DU RESULTAT

Le résultat est transmis au client dès sa validation par l'opérateur de vérification ou le référent fraude le cas échéant. La communication au client de ce résultat est protégée en confidentialité et en intégrité, selon les modalités prévues par la politique de sécurité du système d'information applicable au service.

Le délai maximal entre le début de l'acquisition des données d'identification de l'utilisateur et la notification du résultat au client ne peut excéder quatre-vingt-seize heures.

2.6 GESTION DE LA FRAUDE

Le service de vérification d'identité à distance inclut des mesures de lutte contre les tentatives d'usurpation d'identité, issues notamment de scénarios identifiés dans l'analyse de risque relative au service.

Ces mesures sont ainsi basées sur les indicateurs suivants :

- Qualité de la vidéo ;
- Niveau de ressemblance entre le visage de l'utilisateur issu de la vidéo acquise et la photographie présente sur le titre d'identité présenté ;
- Résultats des vérifications effectuées sur le titre d'identité
- Evaluation du niveau de vraisemblance du caractère vivant de l'utilisateur.

Les mesures effectivement implémentées sont confidentielles, elles ne sont détaillées que dans la déclaration des pratiques de vérification d'identité à distance. Netheos met en œuvre un processus de capitalisation des incidents et fraudes détectés afin d'améliorer continuellement l'efficacité de son service de vérification d'identité à distance.

Chaque usurpation d'identité suspectée ou avérée, qu'elle soit détectée par le service ou communiquée par le service métier de Netheos ou par le client final, génère un alerte incident transmise à l'un des référents fraude Biométrie ou Titre d'identité.

Un utilisateur se considérant victime d'une usurpation d'identité sur le service ou ne parvenant pas à réussir son identification à distance sur le service peut déposer une réclamation selon les modalités décrites à la section suivante.

2.7 GESTION DES RÉCLAMATIONS

Netheos met à la disposition de ces clients et utilisateurs, ainsi que de son service métier interne, un processus d'enregistrement et de traitement des réclamations relatives au service de vérification d'identité à distance.

Des réclamations peuvent par exemple être déposées :

- Par des utilisateurs ou des personnes physiques tierces se considérant victime d'une usurpation d'identité sur le service ;
- Par un utilisateur ne parvenant pas à réussir son identification à distance sur le service ;
- Par un client ayant découvert ou suspecté une usurpation d'identité sur le service ;
- Par un utilisateur ou un client rencontrant un dysfonctionnement sur le service ;
- Par un utilisateur souhaitant annuler une identification frauduleuse en cours ;
- Par un utilisateur souhaitant refuser une identification en cours.

Toute détection ou suspicion d'usurpation d'identité, quelle qu'en soit l'origine, est systématiquement enregistrée et traitée comme une réclamation. Les processus de gestion de fraude exposés au §2.6 sont également activés le cas échéant

L'enregistrement d'une réclamation se déroulent de la manière suivante :

- Pour les clients, au travers dispositif permettant aux clients de remonter les incidents
- Pour les utilisateurs et les tiers :
    - Soit au travers du service de réclamation du client, qui transmettra à Netheos ;
    - Soit directement au point de contact identifié dans la présente politique.

Chaque réclamation fait l'objet d'un traitement par l'expert fraude qui déterminera les actions correctives à moyen et long terme. L'expert fraude pourra, le cas échéant, déclencher la cellule de crise en cas d'incident majeur.

2.8 GESTION DES DONNEES A CARACTERE PERSONNEL

Netheos assure la protection des données à caractère personnel qui sont collectées dans le cadre de l'utilisation du service, en conformité avec la règlementation applicable dont, en particulier, le Règlement Général sur la Protection des Données.

2.8.1 ALTERNATIVE A LA BIOMETRIE

La solution PVID ayant recours à la biométrie, il est obligatoire de proposer à l'utilisateur un parcours alternatif ne faisant pas appel à la biométrie. Ce parcours alternatif est obligatoirement proposé en amont de la procédure d'identification par le service métier ou par le parcours proposé par le client de Netheos.

2.8.2 MINIMISATION ET LISTE DES DONNEES TRAITEES

Le service de vérification d'identité à distance respecte le principe de minimisation des données collectées et conservées. Les données traitées par le service sont les suivantes :

- La vidéo acquise sur le terminal de l'utilisateur et comportant le visage de l'utilisateur et son titre d'identité ;
- Les attributs du titre d'identité ;
- Les traces et informations de connexion de l'utilisateur ;

2.8.3 TRAITEMENT BIOMETRIQUE

Seule la vidéo de l'utilisateur et la photo extraite de la pièce d'identité sont susceptibles de faire l'objet d'un traitement biométrique. Un traitement biométrique est uniquement réalisé pour la finalité de la correspondance du visage et de la reconnaissance du vivant. Une fois l'identité établie, la donnée ne fait plus l'objet de traitement biométrique.

2.8.4 MODALITE DE TRAITEMENT DES DONNEES PERSONNELLES

Nous décrivons les différentes modalités relatives aux données à caractère personnel. Les données personnelles de l'utilisateurs manipulées sont :

- Les vidéos du titre d'identité et de l'utilisateur capturées ;
- Les photos statiques du titre d'identité et du visage extrait des vidéos ;
- Les attributs du titre d'identité extraits de la carte par analyse ;
- Les résultats détaillés des vérifications ;
- Le profil biométrique dérivé ;
- Le résultat global de la vérification retourné au service métier

Ces données, dans le cadre du service PVID, font l'objet de différents traitements ayant des finalités et des durées de conservation différentes. Nous détaillons successivement :

- Les données faisant l'objet d'un traitement biométrique automatisé (§2.8.4.1) ;
- Les données utilisées lors processus de vérification (non biométrique) conservées 96h au maximum (§2.8.4.2) ;
- Les données retournées au service métier (§2.8.4.3) ;
- Les données conservées dans le fichier de preuve (§2.8.4.4) ;
- Les données conservées dans les journaux (§2.8.4.4).

2.8.4.1 DONNEES A CARACTERE PERSONNEL BIOMETRIQUES

Le tableau suivant présente le traitement biométrique des données réalisé pour la correspondance des visages.

Données concernées	Profil biométrique dérivé (profil biométrique calculé sur le visage de la vidéo et de la photo d'identité)
Durée de conservation	Quelques instants le temps de réalisation de l'algorithme.
Modalité de conservation	Non conservées
Modalité de destruction	Effacement automatique de la mémoire après exécution de l'algorithme.

Modalité d'accès	Non accessible hors de l'application (les données sont créées, utilisées par l'application pour établir le verdict puis immédiatement effacées.)
Finalités de conservation	Base légale : • Obligation légale (exigence de contrôle de la correspondance du visage) ;

En tout état de cause, les données biométriques étant immédiatement effacées, elles ne sont pas conservées plus de 96 heures.

2.8.4.2 DONNEES UTILISEES DANS LE CADRE DE LA VERIFICATION D'IDENTITE.

La présente section présente les données utilisées dans le cadre du processus de vérification de l'identité (hors vérification biométrique traité plus haut.

Données concernées	**Vidéos du titre d'identité et de l'utilisateur** **Attributs du titre d'identité** **Photos statiques du titre d'identité et du visage extrait des vidéos** **Résultats détaillés des vérifications.** **Résultat global des vérifications.**
Durée de conservation	Conservation au maximum 96h.
Modalité de conservation	Conservation sur les serveurs sécurisés de Netheos
Modalité de destruction	Destruction automatique du dossier par une méthode d'effacement fiable en fin de période de conservation.
Modalité d'accès	Dossier accessible uniquement des opérateurs et référents de Netheos durant le processus de vérification :
Finalités de conservation	Base légale : • Obligation légale (Nécessité de contrôle de l'identité imposé par le cahier des charges de l'ANSSI)

2.8.4.3 DONNEES RETOURNEES AU SERVICE METIER

Données concernées	**Image extraite de la vidéo du titre d'identité et de l'utilisateur** **Attributs du titre d'identité** **Résultats global des vérifications.**
Durée de conservation	Définie en ligne avec la durée du contrat nécessitant l'identification vidéo en accord avec le guide de conservation de la CNIL.

	Durée de conservation maximum de 96h au sein du service métier de Netheos.
Modalité de conservation	Conservation sous la responsabilité du service métier et le cas échéant du client.
Modalité de destruction	Les données étant transférée au service métier, la modalité de destruction et sont sous la responsabilité du service métier et du client, les données ayant pour finalité d'être intégrées au dossiers et documents du client.
Modalité d'accès	Accessible uniquement au service métier authentifié au travers d'une API. La présente politique interdit l'exercice du droit de rectification ou d'effacement sur les données retournées au service métier
Finalités de conservation	Base légale : • Intérêt légitime de Netheos pour son service de contractualisation en ligne ; • Conservation à des fins de preuve en justice en cas de litige.

2.8.4.4 DONNEES CONSTITUTIVES DU FICHIER DE PREUVE

Données concernées	**Vidéos du titre d'identité et de l'utilisateur** **Attributs du titre d'identité** **Résultats détaillés des vérifications.** **Données retournées au service métier**
Durée de conservation	Durée de conservation de 7 ans après vérification de l'identité.
Modalité de conservation	Conservation sous forme chiffrée dans un dossier de preuve après traitement. Les modalités détaillées du chiffrement sont précisées dans la déclaration des pratiques associées.
Modalité de destruction	Destruction automatique du dossier par une méthode d'effacement fiable en fin de période de conservation. Du fait de l'obligation légale de conserver les données, impossibilité d'exercer a priori le droit à l'oubli et à la rectification durant cette période.
Modalité d'accès	Dossier accessible uniquement des opérateurs de Netheos durant le processus de vérification puis accès uniquement : • Sur réquisition judiciaire • Sur demande d'exercice du droit d'accès de la personne concernée. L'exercice du droit d'accès de l'utilisateur est limité : La présente politique de vérification d'identité à distance interdit l'accès de l'utilisateur aux données ayant fait l'objet de traitements automatisés ou manuels dont la communication est susceptible de renseigner sur

	la nature des vérifications réalisées par le service et relatives à la détection d'usurpation d'identité
Finalités de conservation	Base légale : • Conservation à des fins de preuve en justice en cas de litige • Conservation à des fins de conformité légale aux obligations imposées par le statut de prestataire qualifié ANSSI.

2.8.4.5 DONNEES CONSERVEES DANS LES JOURNAUX

Données concernées	**Journaux applicatifs et systèmes (adresses IP).**
Durée de conservation	Durée de conservation de 10 ans.
Modalité de conservation	Conservation dans le SAE Netheos (archive chiffrée).
Modalité de destruction	Destruction automatique de l'archive par une méthode d'effacement fiable en fin de période de conservation.
Modalité d'accès	Archive accessible uniquement par les équipes de sécurité de Netheos.
Finalités de conservation	• Conservation à des fins de preuve en justice en cas de litige • Conservation à des fins de conformité légale aux obligations imposées par le statut de prestataire qualifié ANSSI • Conservation en cas de diagnostique à la suite d'un incident de sécurité • Conservation en cas de diagnostique à la suite d'un incident sur la donnée personnelle.

3 GESTION DU RISQUE

3.1 APPRECIATION ET TRAITEMENT DES RISQUES

3.1.1 ANALYSE DE RISQUE

Netheos a élaboré

- Une appréciation des risques relatifs à l'usurpation d'identité, conformément à la démarche EBIOS RM ;
- Une appréciation des risques relatifs la sécurité des systèmes d'information conforme à la démarche ISO 27005

Netheos révise les appréciations des risques identifiées à l'exigence annuelle ainsi qu'en cas de changement majeur.

Le profil d'attaquant considéré dans l'analyse de risque est le niveau modéré.

Ces analyses identifient l'ensemble des risques résiduels et sont validées, formellement et par écrit, par la direction de Netheos.

Les analyses de risques sont conservées de façon à assurer leur confidentialité.

3.1.2 TRAITEMENT DU RISQUE

Netheos élabore un plan de traitement des risques portant sur l'intégralité du périmètre du service de vérification d'identité électronique et associés à l'ensemble des appréciations des risques.

L'application du plan de traitement des risques permet de garantir que le service résiste à des attaquants disposant d'un potentiel d'attaque modéré.

Netheos a fait valider, formellement et par écrit, par sa direction le plan de traitement des risques. Netheos établit un suivi périodique de la mise en œuvre du plan de traitement des risques. La direction de Netheos est alertée en cas d'écart significatif. Netheos révise le plan de traitement des risques au minimum annuellement, et en cas de modification de l'une des appréciations des risques identifiées au 3.1.1. Netheos assure la confidentialité du plan de traitement des risques.

Netheos fait valider, formellement et par écrit, par sa direction la politique de sécurité des systèmes d'information.

3.2 PLAN DE TEST DE LA CAPACITE EFFECTIVE DU SERVICE A DETECTER DES TENTATIVES D'USURPATION D'IDENTITE

Netheos élabore et tient à jour un plan de test de l'efficacité des mesures visant à évaluer la capacité effective du service à détecter les tentatives d'usurpation d'identité. Ce plan couvre les périmètres suivants :

- Authenticité du titre ;
- Détection du vivant ;
- Comparaison du visage ;
- Risque relatifs à l'influence sur le comportement de l'utilisateur.

Le plan de test est validé par les référents fraude titre d'identité et biométrie pour chacune des parties les concernant.

Le plan de test est exécuté par Netheos annuellement et à chaque modification structurante du service, mise à jour des appréciations des risques ou du plan de traitement des risques. Les résultats de l'exécution sont consignés dans un rapport et sont validés par les référents fraude biométrie et titre d'identité.

Si les taux mesurés lors de l'exécution du plan de test sont moins bons que les taux cibles définis dans la déclaration des pratiques :

- Les référents sont informés sans délai,
- Un incident est créé et l'ANSSI est notifiée sans délai.

4 PROTECTION DE L'INFORMATION

4.1 TERMINAL

Le service ne nécessite pas l'installation d'une application spécifique sur le terminal de l'utilisateur. Il s'agit d'un service pouvant être appelé depuis une application du commanditaire.
Le service met en œuvre des technologies permettant de réaliser directement la capture des flux vidéo nécessaires, sans rupture. Toute transmission d'un flux vidéo ou d'une partie de flux vidéo réalisé sous le contrôle de l'utilisateur est proscrite.
Le client réalise une veille pour détecter la mise à disposition d'applications frauduleuses visant à se substituer à celle de son application appelant le service Netheos, sur les magasins d'applications officiels.
Netheos protège en confidentialité et en authenticité les données d'identification échangée entre le terminal de l'utilisateur, et le service de vérification d'identité à distance.

4.2 POLITIQUE DE SECURITE DU SYSTEME D'INFORMATION

Netheos définit et met en œuvre une politique de sécurité des systèmes d'information basée sur l'appréciation des risques et le plan de traitement des risques.
Netheos révise la politique de sécurité des systèmes d'information au minimum tous les deux ans, et en cas de modification de l'appréciation des risques ou du plan de traitement des risques

4.3 HOMOLOGATION

Netheos a réalisé une homologation du système d'information du service de vérification d'identité à distance.

Netheos fait valider, formellement et par écrit, par sa direction la décision d'homologation.

4.4 LOCALISATION DES DONNÉES.

Toutes les données relatives au service de vérification d'identité à distance sont exclusivement hébergées et traitées sur le territoire Français. L'exploitation et l'administration du service de vérification d'identité à distance sont exclusivement réalisées depuis le territoire Français.

4.5 NIVEAU DE SÉCURITÉ

Netheos applique au service PVID son socle de sécurité et de pratiques pour ses services de confiance.

Netheos restreint les accès des opérateurs au système d'information du service de vérification d'identité à distance au strict nécessaire pour la réalisation de leurs missions.

Netheos applique également l'ensemble des exigences du Guide d'Hygiène informatique de l'ANSSI pour le niveau standard

4.6 CONTRÔLE

Netheos élabore et met en œuvre un plan de contrôle portant sur l'intégralité du périmètre du service de vérification d'identité à distance. Ce plan de contrôle vise à s'assurer que la politique de sécurité des systèmes d'information et la politique de vérification de l'identité sont appliquées.

Netheos révise le plan de contrôle au minimum annuellement et en cas de modification structurante du système d'information du service de vérification d'identité à distance, notamment celles concernant :

- Son hébergement,
- Son infrastructure et
- Son architecture, ou
- En cas de modification structurante de l'appréciation des risques, du plan de traitement des risques, de la politique de sécurité des systèmes d'information ou de la politique de vérification d'identité à distance

Suite à une évaluation, Netheos :

- Met à jour le plan de traitement des risques pour intégrer les résultats des contrôles ;
- Fait valider par sa direction formellement et par écrit, les résultats des contrôles.

Les résultats des contrôles sont confidentiels et ne sont pas rendus publics.

4.7 SÉCURITÉ PHYSIQUE

Netheos élabore et tient à jour la liste des personnes autorisées à accéder aux locaux hébergeant les systèmes d'information du service de vérification d'identité à distance.

Netheos met en œuvre les mécanismes permettant de garantir que seules les personnes autorisées peuvent accéder aux locaux hébergeant le système d'information du service de vérification d'identité à distance.

En particulier, les accès aux salles serveurs et aux locaux techniques sont contrôlés à l'aide de serrures ou de mécanismes de contrôle d'accès par badge. Les accès non accompagnés des prestataires extérieurs aux salles serveurs et aux locaux techniques sont proscrits, sauf s'il est possible de tracer strictement les accès et de limiter ces derniers en fonction des plages horaires. Une revue des droits d'accès est réalisée régulièrement afin d'identifier les accès non autorisés.

Lors du départ d'un collaborateur ou d'un changement de prestataire, il est nécessaire de procéder au retrait des droits d'accès ou au changement des codes d'accès.

Enfin, les prises réseau se trouvant dans des zones ouvertes au public (salle de réunion, hall d'accueil, couloirs, placards, etc.) doivent être restreintes ou désactivées afin d'empêcher un attaquant de gagner facilement l'accès au réseau de l'entreprise

Netheos met en œuvre les mécanismes permettant de journaliser les accès aux locaux hébergeant le système d'information du service de vérification d'identité à distance.

Netheos définit et met en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des journaux d'accès aux locaux hébergeant le service de vérification d'identité à distance.

4.8 JOURNALISATION

Netheos dispose de journaux pertinents afin de pouvoir détecter d'éventuels dysfonctionnements et tentatives d'accès illicites aux composants du système d'information

En particulier, Netheos a déterminé les composants critiques de son système d'information et a défini la liste des événements à enregistrer.

4.8.1 TYPE D'EVENEMENT A ENREGISTRER

Les événements critiques pour la sécurité sont journalisés.

En particulier, Netheos journalise :

- L'ensemble des traitements automatisés et des actions réalisées par les opérateurs humains dans le cadre d'une vérification d'identité à distance ;
- L'ensemble des accès physiques au locaux hébergeant le système d'information du service de vérification d'identité à distance ;
- Pare-feu : paquets bloqués ;
- Systèmes et applications : authentifications et autorisations (échecs et succès), arrêts inopinés ;
- Services : erreurs de protocoles (par exemples les erreurs 403, 404 et 500 pour les services HTTP), traçabilité des flux applicatifs aux interconnexions (URL sur un relais HTTP, en-têtes des messages sur un relais SMTP, etc.).

4.8.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS

Netheos réalise une corrélation des journaux entre les différents composants du système d'information du service de vérification d'identité à distance.

Netheos procède à une revue par échantillonnage des journaux, et notamment des opérations réalisées par les opérateurs.

4.8.3 PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS

Netheos a défini une politique de conservation des journaux d'événements, qui définit leur politique de conservation.

Les événements critiques pour la sécurité sont conservés au moins 1 ans.

4.8.4 PROTECTION DES JOURNAUX D'EVENEMENTS

Les journaux d'événements font l'objet de mesures de protection permettant d'assurer leur intégrité, leur disponibilité et leur confidentialité.

4.8.5 PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS

Les journaux d'événements sont collectés afin d'assurer leur sauvegarde.

4.8.6 SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS

L'ensemble des traitements automatisés et des actions réalisées par les opérateurs humains dans le cadre d'une vérification d'identité à distance sont centralisés sur un composant du système d'information auquel les opérateurs n'ont pas de droit d'accès.

4.9 SAUVEGARDES

Netheos élabore et met en œuvre un plan de sauvegarde et de restauration des dispositifs du service de vérification d'identité à distance. Ce plan de sauvegarde comporte les volets suivants :

- Sauvegarde des systèmes ;
- Sauvegarde des configurations ;
- Sauvegarde des données.

Netheos teste le plan de sauvegarde et de restauration au minimum une fois par an.

Netheos définit et met en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes effectuées, au même niveau que celui pour lequel le système de vérification a été homologué.

Netheos respecte l'ensemble des mesures et préconisations sur la sécurisation des sauvegardes de la norme [ISO27002].

Le plan de sauvegarde intègre les éléments suivants :

- La liste des données jugées vitales pour l'organisme et les serveurs concernés ;
- Les différents types de sauvegarde ;
- La fréquence des sauvegardes ;
- La procédure d'administration et d'exécution des sauvegardes ;
- Les informations de stockage et les restrictions d'accès aux sauvegardes ;
- Les procédures de test de restauration ;
- La destruction des supports ayant contenu les sauvegardes.

4.10 CLOISONNEMENT

Netheos élabore et maintient à jour une description détaillée de l'architecture du système d'information du service de vérification d'identité à distance.

Le système d'information est dédié exclusivement aux services de confiance de Netheos, dont fait partie le service de vérification d'identité à distance. Toute autre prestation ne mettant pas en œuvre une composante d'un service de confiance est réalisée sur un système d'information cloisonné physiquement du système d'information du service.

Netheos élabore et tient à jour la matrice des flux du système de vérification d'identité à distance, ainsi que la politique de filtrage associée. La politique n'autorise que les flux strictement nécessaires au fonctionnement du service de vérification d'identité à distance.

La matrice des flux (entrants et sortants) est réduite au juste besoin opérationnel, maintenue dans le temps et la configuration des équipements y est conforme.

4.11 ADMINISTRATION ET EXPLOITATION DU SERVICE

Les postes de travail des administrateurs, des opérateurs et des référents fraude sont raccordés exclusivement au système d'information du service de vérification d'identité à distance. En particulier, un poste de travail ou un serveur utilisé pour les actions d'administration n'a en aucun cas avoir accès à Internet.

En cas de besoin d'accès à internet ou à d'autres systèmes d'information, les administrateurs et les opérateurs doivent disposer d'un poste distinct de leur poste de travail, déployé au sein d'une zone externe au système d'information du service de vérification d'identité à distance.

Le réseau d'administration est spécifiquement cloisonné, notamment vis-à-vis du réseau bureautique des utilisateurs, pour se prémunir de toute compromission par rebond depuis un poste utilisateur vers une ressource d'administration (a minima, un cloisonnement logique cryptographique reposant sur la mise en place de tunnels IPsec et de VLA est mis en œuvre).

4.12 INTERCONNEXIONS DU SYSTEME D'INFORMATION DU SERVICE

Netheos identifie dans la description détaillée de l'architecture du système d'information du service de vérification d'identité à distance l'ensemble des interconnexions du système d'information du service de vérification d'identité avec des systèmes d'information tiers, notamment le système d'information du service métier.

Cette interconnexion avec le service métier se fait localement au sein de l'espace sécrisé des services de confiance de Netheos.

Netheos filtre tous les flux aux interconnexions du système d'information du service de vérification d'identité à distance. En particulier, un filtrage IP est réalisé d'un pare-feu au plus près de l'entrée des flux sur le réseau de Netheos.

4.13 ACCÈS DISTANT

Dans le cas où Netheos permettrait des accès à distance de ses collaborateurs au service PVID, les exigences de sécurité préconisées par l'ANSSI pour encadrer ces pratiques seront mises en œuvre chaque fois que cela est applicable.

4.14 DEVELOPPEMENT ET SECURITE DES LOGICELS

Netheos met en place des mesures de développement sécurisé des logiciels mis en œuvre en particulier :

- Le logiciel fait l'objet de revues régulières du code par un autre développeur ;
- Le logiciel doit faire l'objet de tests de non-régression avant mise en production d'une nouvelle version ;
- Le logiciel doit faire l'objet d'un parcours de recettes documenté pour chaque version devant être mise en production ;
- Le logiciel génère des journaux d'enregistrement adaptés pour la corrélation des enregistrements entre les différents processus du service ;
- Les développeurs du logiciel sont sensibilisés aux risques spécifiques liés au domaine de la vérification d'identité, et sont tenus à une obligation de discrétion ;
- Le développement du logiciel doit être réalisé dans des conditions permettant une auditabilité des actions de chaque développeur ;
- Chaque fournisseur de logiciel est tenu d'informer le prestataire de toute fraude interne ou attaque visant à altérer le logiciel fourni ;

- Chaque fournisseur de logiciel est considéré comme un sous-traitant du prestataire pour l'application générale des mesures de protection de l'information.

4.15 GESTION DES incidents

Netheos dispose d'une procédure de gestion des incidents de sécurité. Cette procédure prévoit :

- La notification du référent de sécurité ;
- La consignation de l'incident dans un registre des incidents.

Netheos met en place un processus de gestion de crise en cas d'incident de sécurité majeur affectant le service de vérification d'identité à distance. Netheos informe l'ANSSI sans délai en cas d'incident affectant ou susceptible d'affecter le service de vérification d'identité à distance.

5 ORGANISATION DU PRESTATAIRE ET GOUVERNANCE

5.1 RECRUTEMENT

5.1.1 PROCEDURES DE VERIFICATION DES ANTECEDENTS

La société NETHEOS met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de l'IGC. Cette vérification est basée sur un contrôle des antécédents de la personne, il est vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions, par la demande d'un extrait du bulletin n°3 du casier judiciaire.

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

Une vérification des formations, qualifications, références professionnelles des candidats (opérateurs, référents fraude, etc.) pour le service de vérification d'identité à distance et de la véracité de leur curriculum vitae préalablement à leur embauche.

5.1.2 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 du service en fonction de leur version ;
- Procédures applicables pour les services ;
- Responsabilités du rôle ;
- Procédures pour la résolution des incidents et des litiges ;
- Connaissance minimale du système informatique ;
- Procédure du plan de continuité.

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

Les équipes opérationnelles, pour être à l'état de l'art de la sécurité des systèmes d'information, suivent, à leur prise de poste, des formations sur :

- La législation en vigueur ;
- Les principaux risques et menaces ;
- Le maintien en condition de sécurité ;
- L'authentification et le contrôle d'accès ;
- Le paramétrage fin et le durcissement des systèmes ;
- Le cloisonnement réseau ;
- Et la journalisation.

Après le recrutement, Netheos sensiblise également les opérateurs et référents fraude aux risques spécifiques relatifs à leur fonction, et les informer de leur obligation de discrétion

5.2 CHARTE D'ETHIQUE

Netheos dispose d'une charte d'éthique intégrée au règlement intérieur, prévoyant notamment que :

- Les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- Les personnels ne recourent qu'aux méthodes, outils et techniques validés par le Netheos ;
- Les personnels s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation sauf autorisation formelle, écrite et authentifiée du commanditaire ;
- Les personnels s'engagent à signaler au prestataire tout contenu illicite découvert pendant la prestation ;
- Les personnels s'engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.

Netheos fait signer à l'ensemble de son personnel la charte d'éthique et préalablement à la réalisation de la prestation.
Netheos veille au respect de la charte d'éthique et prévoit des sanctions disciplinaires à l'intention des opérateurs, des administrateurs et des experts du service de vérification ayant enfreint les règles de sécurité ou la charte d'éthique.

5.3 ORGANISATION ET GESTION DES COMPÉTENCES

5.3.1 NOMBRE DE PERSONNES REQUISES PAR TACHE

Netheos emploie un nombre suffisant d'opérateurs, de référents biométrie et de référents Fraude Titre assurant les missions et disposant des compétences identifiées pour assurer totalement et dans tous ses aspects le service de vérification d'identité à distance.

5.3.2 DOCUMENTATION FOURNIE AU PERSONNEL

Netheos fournit au personnel en charge du service les documentations nécessaires en fonction de leur attribution.

En particulier, Netheos met à disposition des opérateurs et des référents Fraude l'ensemble du matériel pédagogique et technique qui leur permettent de remplir les missions qui leurs sont confiée

5.3.3 FORMATION CONTINUE

Netheos élabore et met en œuvre un plan de formation régulier des opérateurs et des référents Fraude en adéquation avec les missions et compétences identifiées.

En particulier, à intervalles réguliers, les équipes doivent suivre des formations complémentaires sur les sujets évoqués au 5.1.2

Ces formations sont complétées d'actions de sensibilisation régulières, adaptées aux utilisateurs ciblés et pouvant prendre différentes formes (mails, affichage, réunions, espace intranet dédié, etc.).

5.3.4 PLAN DE CONTROLE

Netheos élabore et met en œuvre un plan de contrôle régulier afin de vérifier que les opérateurs et référents Fraude disposent des compétences identifiées.

Netheos prévoit que chaque opérateur et référent Fraude, préalablement à la réalisation de la prestation, a bien suivi le plan de formation et réussi le plan de contrôle.

5.3.5 BULLETIN OPERATIONNEL

Netheos fait figurer dans les bulletins opérationnels au minimum :

- Les indicateurs opérationnels du service (voir section 6);
- Une revue des réclamations reçues, en cours de traitement ou clôturées ;
- Une revue des incidents de sécurité détectés sur le système d'information du service de vérification d'identité à distance ;
- Une revue des incidents de sécurité notifiés à l'ANSSI ;
- La date de la dernière exécution du plan de test ;
- Les taux de faux positifs et négatifs mesurés pour la vérification de l'authenticité des titres, la détection du vivant et la correspondance des visages ;
- Une revue des alertes générées par le service de vérification d'identité à distance ;
- Les modifications apportées au service de vérification d'identité à distance ;
- Les modifications apportées à la politique de vérification d'identité à distance ;
- Les modifications apportées à l'analyse de risques, notamment si la liste des scénarios de risque est modifiée

La service PVID de Netheos partage le bulletin opérationnel avec le service métier de Netheos sur une base mensuelle. Celui-ci est ensuite partagé avec les clients utilisateurs sur une base similaire. Le bulletin est transmis de façon confidentielle au service métier et aux destinataires clients via l'outil de support de Netheos.

5.3.6 RELATION AVEC LES SERVICES DE L'ETAT

Netheos a nommé un officier de sécurité chargé notamment d'assurer la liaison avec les services de l'État compétents en cas de fraude ou d'attaque

5.4 RÔLES DE CONFIANCE

Netheos a défini les rôles de confiance suivants :

- Administrateur ;
- Opérateur ;
- Référent fraude biométrie ;
- Référent fraude titre d'identité ;
- Officier de sécurité.

L'ensemble des personnels en rôle de confiance sont établis en France métropolitaine.

5.4.1 ADMINISTRATEUR

Il est en charge de l'administration et de la configuration de l'ensemble des composants techniques du service ainsi que des opérations d'exploitation quotidienne du service. Il est autorisé à réaliser des sauvegardes et des restaurations.

5.4.2 OPERATEUR

5.4.2.1 MISSION

L'agent assure les missions suivantes :

- Vérifier, conformément à la présente politique de vérification d'identité, l'identité des utilisateurs sur la base des données d'identification relatives aux utilisateurs acquises, des résultats des traitements automatisés réalisés sur ces données d'identification ;
- Prononcer le verdict « succès » ou « échec » relatif à la vérification d'identité à distance et générer une alerte à chaque suspicion de détection ou détection d'une usurpation ou altération d'identité.

5.4.2.2 COMPETENCES ET CONNAISSANCES

L'agent dispose des compétences suivantes :

- Connaître et appliquer la politique de vérification d'identité à distance ;
- Connaître et appliquer la politique de sécurité des systèmes d'information ;
- Connaître l'état de la menace relative à l'usurpation d'identité ;
- Connaître et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment le [RGPD] ;
- Connaître les modes opératoires des attaquants permettant d'aboutir aux scénarios de risques identifiés dans l'appréciation des risques, et notamment ceux relatifs aux titres d'identité et à la biométrie ;
- Être physionomiste, reconnaître et comparer des visages sur des supports photo et vidéo ;
- Connaître les éléments de sécurité des titres d'identité ainsi que les vérifications à réaliser pour identifier de faux titres d'identité ou des titres d'identité altérés ;
- Connaître et maîtriser l'utilisation du registre PRADO.

5.4.3 REFERENT FRAUDE BIOMETRIE

5.4.3.1 MISSION

Le référent fraude Biométrie assure les missions suivantes :

- Valider formellement les modifications de la politique de vérification d'identité à distance lorsque ces modifications sont relatives à la biométrie ;
- Traiter les escalades générées par les opérateurs lorsqu'ils suspectent ou détectent une occurrence d'un scénario de risque identifié dans l'appréciation des risques et relatif à la biométrie ;
- Traiter les alertes générées lorsqu'un opérateur a proposé un verdict de la vérification d'identité à distance à «succès» alors que les traitements automatisés suspectent ou détectent une fraude relative à la biométrie ;
- Assurer la formation des opérateurs aux vérifications relatives à la biométrie, et notamment à la vérification des données d'identification biométriques, à la comparaison de visages ;
- Assurer la formation des opérateurs aux modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques d'usurpation d'identité relatifs à la biométrie ;
- Contrôler que les opérateurs disposent des compétences attendues relatives à la biométrie ;
- Valider formellement les modifications de la politique de vérification d'identité à distance lorsque ces modifications sont relatives à la biométrie ;
- Valider la conception et l'implémentation des vérifications relatives à la biométrie réalisées par traitement automatisé.

5.4.3.2 COMPETENCES ET CONNAISSANCES

Le référent fraude Biométrie dispose des compétences suivantes :

- Connaître et appliquer la politique de vérification d'identité à distance ;
- Connaître et appliquer la politique de sécurité des systèmes d'information ;
- Connaître l'état de la menace relative à l'usurpation d'identité ;
- Maîtriser l'état de la menace relative à la biométrie ;
- Connaître et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment [RGPD] ;
- Maîtriser les modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques et relatifs à la biométrie ;
- Maîtriser les vérifications à réaliser pour identifier les occurrences des scénarios de risque identifiés dans l'appréciation des risques et relatifs à la biométrie ;
- Connaître et appliquer les procédures relatives aux alertes générées par un opérateur lorsqu'il suspecte ou détecte une occurrence d'un scénario de risque identifié dans l'appréciation des risques et relatif à la biométrie ;

- Connaître et appliquer les procédures relatives aux alertes générées lorsqu'un opérateur propose un verdict de la vérification d'identité à distance à « succès » alors que les traitements automatisés suspectent ou détectent une fraude relative à la biométrie.

5.4.4 REFERENT FRAUDE TITRE

5.4.4.1 MISSION

Le référent fraude Titre d'identité assure les missions suivantes

- Valider formellement les modifications de la politique de vérification d'identité à distance lorsque ces modifications sont relatives aux titres d'identité ;
- Traiter les escalades générées par les opérateurs lorsqu'ils suspectent ou détectent une occurrence d'un scénario de risque identifié dans l'appréciation des risques et relatif au titre ;
- Traiter les alertes générées par les opérateurs lorsqu'ils suspectent ou détectent un scénario de risque identifié dans l'appréciation des risques et relatif au titre d'identité ;
- Traiter les alertes générées lorsqu'un opérateur a proposé un verdict de la vérification d'identité à distance « succès » alors que les traitements automatisés suspectent ou détectent une fraude relative au titre d'identité ;
- Assurer la formation des opérateurs aux vérifications relatives aux titres d'identité, et notamment aux contrôles des éléments de sécurité des titres d'identité afin d'identifier les faux titres d'identité ou les titres d'identité altérés ;
- Assurer la formation des opérateurs aux modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques d'usurpation d'identité relatifs aux titres d'identité ;
- Contrôler que les opérateurs disposent des compétences attendues relatives aux titres d'identité

5.4.4.2 COMPETENCES ET CONNAISSANCES

Le référent fraude Titre d'identité dispose des compétences suivantes

- Connaître et appliquer la politique de vérification d'identité à distance ;
- Connaître et appliquer la politique de sécurité des systèmes d'information ;
- Maîtriser l'état de la menace relative aux faux titres d'identité ;
- Connaître et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment le [RGPD].

5.4.5 OFFICIER DE SECURITE

Dans le cadre de la présente politique, l'officier de sécurité est chargé d'assurer la liaison avec les services de l'Etat compétent en cas de fraude ou d'attaque.

Il est également un référent en sécurité des systèmes d'information qui sera soutenu par la direction. Ce référent est connu de tous les utilisateurs et est le premier contact pour toutes les questions relatives à la sécurité des systèmes d'information :

- Définition des règles à appliquer selon le contexte ;
- Vérification de l'application des règles ;

- Sensibilisation des utilisateurs et définition d'un plan de formation des acteurs informatiques ;
- Centralisation et traitement des incidents de sécurité constatés ou remontés par les utilisateurs.

Ce référent est formé à la sécurité des systèmes d'information et à la gestion de crise.

6 QUALITE ET NIVEAU DE SERVICE

6.1 QUALITÉ DU SERVICE

Netheos élabore et met en œuvre un processus de capitalisation des incidents et fraudes détectés afin d'améliorer continuellement l'efficacité de son service de vérification d'identité à distance.

Netheos, en tant que fournisseur de service et commanditaire du service, les indicateurs opérationnels du service de vérification d'identité à distance. Ces indicateurs comportent à minima :

- Le temps moyen, minimal et maximal d'attente des utilisateurs ;
- Le nombre de vérifications d'identité à distance réalisées, quels que soient les résultats de ces vérifications ;
- Le nombre de vérifications d'identité à distance selon les résultats de ces vérifications (succès ou échec) ;
- Le nombre de vérifications d'identité à distance en échec, selon la nature de la vérification (vérification de l'authenticité du titre, comparaison du visage de l'utilisateur avec la photo du titre d'identité, vérification du vivant) ;
- Le nombre de tentatives d'usurpation d'identité détectées par le prestataire, selon la nature de la tentative (faux titre d'identité, etc.) ;
- Le nombre d'usurpations d'identité identifiées par le service métier et communiquées par le service métier au prestataire ;
- Le nombre des plaintes relatives au service de vérification d'identité à distance reçues ;
- Le nombre des plaintes relatives au service de vérification d'identité à distance traitées et qui ont donné lieu à une action corrective du service ;
- Le nombre des plaintes relatives au service de vérification d'identité à distance traitées et qui n'ont pas donné lieu à une action corrective du service.

Netheos élabore et tient à jour un processus de mesure des indicateurs décrivant, pour chacun des indicateurs opérationnels, les méthodes et moyens mis en œuvre par le prestataire pour mesurer l'indicateur.

6.2 CONVENTION DE SERVICE

Netheos étant à la fois commanditaire et prestataire, il n'est pas formellement établi de convention de service. Les exigences du cahier des charges ANSSI relatives à la convention de service sont cependant reprises dans le contrat liant Netheos à ses clients ayant recours au service PVID.

7 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Pour s'assurer du niveau de sécurité de son infrastructure interne et du service de vérification d'identité à distance, NETHEOS a mis en place un processus d'audit interne, en plus du processus d'évaluation du service décrit dans le cahier des charges de l'ANSSI.

D'autres audits externes seront réalisés sur le périmètre, commun à plusieurs services de confiance 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.

7.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

La fréquence des audits s'établit comme suit :

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

7.2 IDENTITES ET QUALIFICATION DES EVALUATEURS

L'équipe d'audit système est constituée d'experts internes à la société Netheos spécialistes du domaine de la sécurité. Netheos peut également avoir recours à des sociétés externes spécialistes du domaine audité.

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.

7.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

L'équipe d'auditeur est composée de personnes neutres. Celles-ci n'ont aucune fonction opérationnelle ou fonction de sécurité sur les composantes qu'ils auditent.

7.4 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 la Direction de Netheos 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 la Direction qui peuvent être la cessation (temporaire ou définitive) d'activité, la notification a posteriori d'une fraude , etc. Le choix de la mesure à appliquer est effectué par le service PVID de Netheos et doit respecter ses politiques de sécurité internes ;

- Avec réserve, Netheos 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, Netheos confirme à la composante contrôlée la conformité aux exigences de la présente politique et de la déclaration des pratiques associée.

7.5 COMMUNICATION DES RÉSULTATS

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

8 AUTRES PROBLEMATIQUES METIERS ET LEGALES

8.1 TARIF

La vérification d'identité est facturée à la transaction.

8.2 RESPONSABILITÉ FINANCIÈRE

8.2.1 COUVERTURE PAR LES ASSURANCES

Netheos a souscrit une assurance responsabilité civile couvrant les risques liés à son activité professionnelle.

8.2.2 AUTRES RESSOURCES

Netheos engage les ressources financières nécessaires pour assurer ses activités et notamment la gestion de la fin de vie du service. Cela comprend notamment les ressources permettant de maintenir la conservation des dossiers de preuve.

8.2.3 COUVERTURE ET GARANTIE CONCERNANT LES ENTITES UTILISATRICES

Sans objet.

8.3 CONFIDENTIALITÉ DES DONNÉES PROFESSIONNELLES

8.3.1 PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Les informations suivantes sont considérées comment confidentiels :

- Les vidéos et données d'identité capturées par le service ;
- Les données biométriques calculées par le service ;
- Les résultats des différentes vérifications, humaines et automatisées, réalisées par le service ;
- Les dossiers de preuve ;
- Les journaux d'événements ;
- Les rapports d'audits ;
- Les déclarations des pratiques associées au présent document ;

- Le corpus documentaire associé au présent document.

8.3.2 INFORMATIONS HORS DU PERIMETRE DES INFORMATIONS CONFIDENTIELLES

Le présent document, les CGUs et de façon plus générale l'ensemble des données sur le site de publication sont publiques.

8.3.3 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.

8.4 PROTECTION DES DONNÉES PERSONNELLES

8.4.1 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.

8.4.2 INFORMATIONS A CARACTERE PERSONNEL

Voir 2.8.

8.4.3 INFORMATIONS A CARACTERE NON PERSONNEL

Sans objet.

8.4.4 RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES

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

8.4.5 NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES

Netheos recueille le consentement explicite pour utiliser les données personnelles, en particulier les données biométriques.

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

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

8.4.7 AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES

Les utilisateurs peuvent exercer leur droit d'accès à leurs données à caractère personnel, conformément au RGPD, dans les limites décrites dans la présente politique.

8.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

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

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

8.6 INTERPRÉTATIONS CONTRACTUELLES ET GARANTIES

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

8.6.1 OBLIGATIONS DU SERVICE PVID

NETHEOS en tant que prestataire s'engage à :

- Respecter la présente politique, la déclaration des pratiques associées et les CGU ;
- Rendre disponible les CGU à l'Utilisateur avant le processus de vérification d'identité et, le cas échéant, la signature des Documents Métier ;
- Informer l'Utilisateur du pays dans lequel se trouve les opérateurs chargés de réaliser les vérifications et de prononcer le verdict de la vérification d'identité à distance ;
- À collecter les données et pièces justificatives permettant de valider l'identité de l'Utilisateur ;
- Alerter les Clients en cas d'incident de sécurité ayant des conséquences sur le processus de vérification d'identité à distance ;
- Protéger les données personnelles des Utilisateurs ;
- Mettre en place, chaque fois que cela est possible, des pratiques de vérification d'identité qui sont non discriminatoires ;
- Vérifier avec diligence l'identité des utilisateurs, conformément aux engagements de la présente politique et de la déclaration des pratiques ;
- Traiter dans les meilleurs délais les réclamations et les litiges ;
- En cas de cessation définitive du service, Netheos s'engage à archiver les journaux et les dossiers de preuves associés aux Clients.

8.6.2 OBLIGATIONS DES UTILISATEURS DU SERVICE

Les utilisateurs du service doivent :

- S'engager à respecter l'ensemble des engagements des CGUs ;
- Accepter l'utilisation de procédés biométriques ;
- Fournir une pièce d'identité valide et acceptée par le service

- Respecter les indications fournies à l'écran pour maximiser la réussite du parcours

8.7 LIMITE DE GARANTIE

Sans objet.

8.8 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 Politique 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.

8.9 INDEMNITÉS

Sans objet.

8.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PRESENTE POLITIQUE

8.10.1 DUREE DE VALIDITE

Cette politique reste en application jusqu'à la publication d'une nouvelle version et reste applicable pour toutes les vérifications d'identité réalisée durant sa période de validité.

8.10.2 FIN ANTICIPEE DE VALIDITE

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

8.10.3 EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES

Sans objet.

8.10.4 NOTIFICATIONS INDIVIDUELLES ET COMMUNICATIONS ENTRE LES PARTICIPANTS

Netheos met à disposition la nouvelle version de la politique dès qu'elle est validée par le C2SSC.

8.11 AMENDEMENTS A LA POLITIQUE

8.11.1 PROCEDURES D'AMENDEMENTS

Le C2SSC révise cette politique au moins une fois par an. D'autres révisions peuvent être décidées à tout moment à la discrétion du C2SSC.

8.11.2 MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS

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

8.11.3 CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE

L'OID de la politique de sur service PVID permet d'identifier le service de façon unique, toute évolution de cette politique ayant un impact majeur (par exemple, changement de niveau d'exigence du service.) 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 politique doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente politique) intervient dans les exigences de la présente politique applicable au service considéré.

8.12 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 politique 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.

8.13 JURIDICTIONS COMPÉTENTES

Se reporter au § 8.12.

8.14 CONFORMITÉ AUX LÉGISLATIONS ET RÉGLEMENTATIONS

Netheos se conforme à la législation et la réglementation en vigueur sur le territoire français.

Comme évoqué en introduction, le service se conforme au cahier des charges PVID en vigueur pour le niveau substantiel.

8.15 DISPOSITION DIVERSES

8.15.1 ACCORD GLOBAL

Sans objet.

8.15.2 TRANSFERT D'ACTIVITES

Sans objet.

8.15.3 CONSEQUENCES D'UNE CLAUSE NON VALIDE

Sans objet.

8.15.4 APPLICATION ET RENONCIATION

Sans objet.

8.16 FORCE MAJEURE

NETHEOS ne pourra être tenu pour responsable, ou considéré comme ayant failli aux conditions de la présente politique, 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

8.17 AUTRES DISPOSITIONS

Sans objet.