Politique de vérification d'identité à distance (PVID)

Version 1.4

IDnow GmbH
Auenstr. 100
80469 Munich

06.07.2023

Politique de vérification d'identité à distance d'IDnow

Version	1.4
Date	06.07.2023
Auteur	Armin Bauer, IDnow GmbH (armin.bauer@idnow.io)
Classification	Public, publié sur https://www.idnow.io/certification-policies/
Politique de sécurité	Politique de sécurité d'IDnow, version 1.6
Politique d'infrastructure du centre d'identification	Politique d'infrastructure du centre d'identification IDnow, version 1.0
Politique d'infrastructure des centres de données	Politique relative à l'infrastructure du centre de données d'IDnow, version 1.1
Évaluation des risques Signature électronique qualifiée VideoIdent	Signature électronique d'évaluation des risques qualifiée IDnow VideoIdent, version 1.1
Politique de l'OID	Politique d'IDnow en matière d'OID 1.0
Norme PVID de l'ANSSI	Référentiel d'exigences applicables aux prestataires de vérification d'identité à distance publié par l'ANSSI, Version 1.1 du 1er mars 2021 Disponible sur https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf
[HYGIÈNE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NT_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[NOMADISME]	Recommandations sur le nomadisme numérique, ANSSI, référence ANSSI-PA-054, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B1]	Règles et recommandations concernant les mécanismes d'authentification, ANSSI. Disponible sur http://www.ssi.gouv.fr

Historique		
Date	Version	Commentaire
06/07/2023	1.4	• 1.4.2 : Correction d'une référence erronée à l'annexe • 2.3, 2.4 : ajout d'une clarification concernant le processus de changement • 2.9 : Retirée et mise à jour des sections connexes • 5 : Clarification sur le fait que la certification est valable au maximum 2 ans OID: 1.3.6.1.4.1.56907.2.1.4.1.5
21/06/2023	1.3	• Ajout de la liste des documents acceptés OID: 1.3.6.1.4.1.56907.2.1.4.1.4
06/04/2023	1.2	• Diviser le document en une version spécifique à VideoIdent et AutoIdent

		OID: 1.3.6.1.4.1.56907.2.1.4.1.3
13/04/2022	1.1	• Clarification concernant la confidentialité du document • Clarification concernant les documents acceptés OID-V: 1.3.6.1.4.1.56907.2.1.4.1.2 OID-A: 1.3.6.1.4.1.56907.2.2.4.1.2
31/03/2021	1.0	Création du document. OID-V: 1.3.6.1.4.1.56907.2.1.4.1.1 OID-A: 1.3.6.1.4.1.56907.2.2.4.1.1

Table des matières

1. OBJET DU DOCUMENT

IDnow GmbH agit en tant que prestataire de vérification d'identité à distance qualifié conformément aux exigences et au processus d'évaluation de l'ANSSI. IDnow effectue uniquement la vérification d'identité à distance d'une personne physique (également appelée Utilisateur dans le présent document). L'Utilisateur est en relation avec un Opérateur d'IDnow à l'aide d'un ordinateur ou d'un téléphone portable et d'un document d'identité. IDnow procède ensuite à une seconde vérification manuelle pour donner le résultat de l'identification. Il s'agit d'un "service de vérification d'identité à distance synchrone avec interaction humaine" tel que défini dans la norme PVID 1.1. Le présent document constitue la politique complète de vérification d'identité à distance (PVID) pour les deux processus. L'OID de ce service est :

- OID: 1.3.6.1.4.1.56907.2.1.4.1.5

La dernière section de l'OID ("E") indique la version de la politique. Veuillez consulter le tableau des versions au début du document pour connaître l'OID complet des versions précédentes. Veuillez également consulter la politique d'IDnow en matière d'OID pour comprendre comment les OID sont mis en place. Les services sont vendus à un client (nommé "Commanditaire" dans la norme ANSSI).

Le service est conforme au niveau d'assurance Substantiel tel que défini par l'ANSSI dans la norme PVID.

La présente PVID est complétée par une déclaration sur les pratiques de vérification de l'identité à distance (DPVID) qui est confidentielle et n'est pas communiquée à l'Utilisateur ou à la partie se fiant à l'information, mais uniquement aux personnes qui ont besoin d'en avoir connaissance.

La PVID dispose d'un contact identifié au point 1.5.2. Cette personne est chargée des tâches suivantes :

- Signaler tous les incidents de sécurité au client,
- Gérer les changements au sein de ce document lors de la validation de l'ANSSI,
- Contrôler que les procédures opérationnelles concernant les activités des clients sont exécutées conformément au présent PVID.

IDnow suit les quatre étapes suivantes pour s'assurer que l'identification d'une personne physique en ligne présente une "garantie équivalente" à celle d'une identification en personne :

1) Vérification de l'existence réelle de la personne dans la vie réelle ("Liveness Detection")
2) Vérifier si le document d'identité appartient à cette personne spécifique
3) Preuve que la personne présente est la même que celle indiquée dans le document d'identité
4) Vérifier l'authenticité du document d'identité

IDnow, agissant principalement en tant que fournisseur de vérification d'identité à distance, agit au nom de :

- Une partie utilisatrice (client commanditaire, par exemple un établissement financier) pour transmettre à l'Utilisateur des documents qui nécessitent sa signature.

- pour le compte de l'utilisateur en tant que politique d'enregistrement (RA), en effectuant un face à face à distance comme indiqué dans l'article 24 d'eIDAS pour demander un certificat qualifié à délivrer par l'autorité de certification,
- au nom de l'utilisateur en tant que mandataire pour demander la signature électronique d'un ou de plusieurs documents joints à la demande,
- au nom de la partie se fiant à la loi en tant qu'agent, reçoit les documents signés, effectue tous les contrôles requis par la loi applicable et crée un rapport de qualité permettant à la partie se fiant à la loi d'identifier le nouveau client conformément à la loi,
- au nom de l'AC comme point de contact pour entamer une procédure de révocation

Cette Politique de Vérification d'Identité à Distance fait référence :

- à la politique de sécurité d'IDnow,
- à la politique d'infrastructure du centre d'identification d'IDnow,
- à la politique d'infrastructure du centre de données d'IDnow,
- ainsi qu'aux évaluations des risques et à la norme de l'ANSSI utilisée pour certifier les services.

Ils fournissent des détails supplémentaires mais ont été retirés de la Politique de Vérification d'Identité à Distance en raison de la sensibilité de leur contenu. La version correcte de ces documents pour cette Politique de Vérification d'Identité à Distance est mentionnée au début de ce document.

Les évaluations des risques d'IDnow sont conformes à la norme ISO 27005 et tiennent compte des risques liés à l'usurpation d'identité et à la sécurité du système informatique utilisé pour les services VID. Les évaluations des risques sont révisées chaque année conformément au référentiel d'exigences PVID de l'ANSSI et à la suite de changements majeurs tels que définis dans ces documents. Dans son analyse des risques, IDnow considère les profils d'attaquants suivants : toute personne, groupe de personnes ou organisation malveillante, interne ou externe, ayant un potentiel d'attaque modéré.

L'analyse des risques contient un plan de traitement des risques et un plan d'essai pour tester la capacité effective du service à détecter les tentatives d'usurpation d'identité.

La présente politique est définie sur la base de l'analyse des risques d'IDnow en tenant compte des exigences de l'ANSSI. La Déclaration des Pratiques de Vérification d'Identité à Distance en donne les détails.

En outre, la présente politique est complétée par la politique de sécurité d'IDnow qui couvre tous les aspects du référentiel d'exigences PVID de l'ANSSI. IDnow revoit sa politique de sécurité au moins une fois par an, et en cas de modification de l'évaluation des risques ou du plan de traitement des risques d'IDnow.

Le contact identifié dans la présente politique valide l'analyse de risque d'IDnow,la politique de sécurité d'IDnow et la signe dans le cadre du processus d'homologation demandé par l'ANSSI. Les services de Vérification d'Identité à Distance (VID), tels que définis dans la présente politique, ne peuvent être exécutés qu'après homologation officielle par IDnow et certification par l'ANSSI.

1.2. PARTICIPANTS

IDnow fait appel à un fournisseur pour l'exploitation du centre de données. Le fournisseur met à disposition le matériel serveur, les racks, le pare-feu, l'électricité, l'internet, etc. IDnow prend ensuite le relais au niveau du matériel (système d'exploitation et couches supérieures).

IDnow a deux contacts principaux avec l'opérateur des centres de données : Un contact pour les questions commerciales/contractuelles et un autre pour les questions techniques.

En outre, il existe une ligne téléphonique d'urgence technique permettant à IDnow de contacter directement le fournisseur du centre des données.

Il existe également un système de notification (par exemple, une liste de diffusion) fourni par les exploitants des centres de données, qui informe IDnow des travaux de maintenance à venir.

Un contrat régit les relations commerciales entre les exploitants de centres de données et IDnow. L'étendue des services fournis est réglementée dans ce contrat. Il existe également un accord de traitement des données avec le détail des mesures techniques et organisationnelles correspondantes.

Les détails peuvent être trouvés dans le document "IDnow Security Policy", section 8.4 et dans le document "IDnow Data Center Infrastructure Policy", section 3.

Outre son propre centre d'identification, IDnow s'associe à d'autres fournisseurs de centres d'appel pour fournir le service d'identification.

Pour améliorer la qualité de la reconnaissance des visages et de la détection du caractère vivant, IDnow utilise des SDK d'experts dans ces domaines.

Il existe des contrats pour tous les sous-traitants qui régissent l'étendue des services et des responsabilités. Les contrôles mis en œuvre qui sont nécessaires pour fournir ce service sont documentés dans la "Politique d'infrastructure du centre d'identification IDnow", section 3, et font partie du contrat.

1.3. ADMINISTRATION DE LA POLITIQUE

1.3.1. GESTION DU DOCUMENT

Ce document est publié et mis à jour par IDnow GmbH, Allemagne. IDnow met sa politique de vérification d'identité à distance à la disposition du public sur son site web à l'adresse https://www.idnow.io/certification-policies/.

Elel est revue régulièrement, au moins une fois par an ou sur la base de changements, et approuvée par un membre du conseil d'administration. Le responsable de la sécurité informatique est chargé de la mise en œuvre des pratiques. Les modifications apportées au document seront publiées sur le site web d'IDnow après approbation du conseil d'administration.

La présente politique est rédigée selon le référentiel d'exigences PVID de l'ANSSI et selon les résultats de l'analyse de risque d'IDnow.

L'évaluation des risques d'IDnow VideoIdent Qualified Electronic Signature fournit une analyse des scénarios d'attaque et de leurs contre-mesures dans le chapitre Annexe A : Matrice des menaces.

1.3.2. POINT DE CONTACT

Adresse :

IDnow GmbH
Auenstr. 100
80469 Munich
Allemagne

Contact :

Portail du Service Desk (24x7) : https://support.idnow.de
Téléphone (9h00 - 18h00, priorité basse et moyenne uniquement) : +49 89 413 24 600 (sélectionnez la langue -> appuyez sur 3)
Courriel (de 9 h à 18 h, priorité faible et moyenne uniquement) : tickets@idnow.de.

IDnow désigne un responsable de la sécurité qui a notamment pour mission d'assurer la liaison avec les administrations concernées et l'ANSSI en cas de fraude ou d'attaque.

1.4 DÉFINITIONS ET ACRONYMES

1.4.1 ACRONYMES

ANSSI : Agence nationale de la sécurité des systèmes d'information

OID : Identificateur d'objet

PASSI : Prestataire d'audit de la sécurité des systèmes d'information (laboratoire accrédité pour auditer IDnow par rapport au référentiel d'exigences PVID de l'ANSSI et au présent PR).

PRADO : Public Register of Authentic Travel and Identity Documents Online3 - Registre public en ligne de documents authentiques d'identité et de voyage

IT : Technologies de l'information

eIDAS : Electronic Identification, Authentification and Trust Services - Règlement européen n°910/2014 sur l'identification électronique et les services de confiance

RGPD : Règlement général sur la protection des données

FAR : False Acceptance Rate - Taux de faux positifs (acceptation à tort)

FRR : False Rejection Rate - Taux de faux négatifs (rejets à tort)

1.4.2 DÉFINITIONS

Les définitions ci-dessous s'appliquent à ce document. Certaines d'entre elles sont basées sur les règlements européens [EIDAS] et [RGPD].

Administrateur - personnel du service de vérification d'identité à distance disposant de droits d'accès privilégiés à tout ou partie des éléments du système d'information du service de vérification d'identité à distance.

Attributs d'identité - un sous-ensemble des données d'identification transmises par le service de vérification d'identité à distance au service commercial.

Client - l'entité responsable d'un service commercial qui utilise un service de vérification d'identité à distance.

Composant de sécurité - le composant électronique d'un document d'identité, utilisé comme support de stockage sécurisé pour les données d'état civil et la photographie du détenteur légitime du document. L'accès aux informations contenues dans le composant de sécurité d'un document d'identité peut être restreint en vertu du droit national.

Composant du système d'information - tout élément logiciel ou matériel du système d'information impliqué dans la fourniture du service de vérification d'identité à distance.

Consentement - toute manifestation de volonté libre, spécifique, informée et univoque par laquelle l'utilisateur accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel le concernant fassent l'objet d'un traitement.

Résultat intermédiaire de la vérification d'identité à distance - information générée par le service de vérification d'identité à distance dans le cadre des analyses effectuées par le traitement automatique ou par l'opérateur, et nécessaire au verdict de la vérification d'identité à distance. Plusieurs résultats intermédiaires peuvent contribuer à un seul verdict.

Accord de service - accord écrit ou contrat entre un fournisseur de services de vérification d'identité à distance et un client pour l'exécution du service. Si le prestataire est une organisation privée, l'accord de service désigne le contrat.

Déclaration des pratiques de vérification de l'identité à distance - l'ensemble des pratiques (organisation, procédures opérationnelles, ressources techniques et humaines, etc.) que le prestataire de vérification de l'identité à distance applique dans le cadre de la fourniture du service et conformément à la politique de vérification de l'identité à distance à laquelle il s'est engagé. La déclaration des pratiques de vérification de l'identité à distance est confidentielle et n'est mise à la disposition que des personnes ayant le besoin d'en connaître.

Détection en direct - la détection du caractère "en direct" de l'utilisateur vise à authentifier la vidéo du visage de l'utilisateur, afin de vérifier qu'elle n'a pas été modifiée physiquement ou numériquement.

Données d'identification - ensemble de données personnelles acquises et vérifiées par le service afin de vérifier l'identité d'une personne physique. Dans le contexte de la présente PVID, les données d'identification peuvent être la vidéo du visage de l'utilisateur, la vidéo de la pièce d'identité présentée par l'utilisateur ou les données de l'utilisateur (y compris l'image faciale de l'utilisateur) stockées dans le composant de sécurité de la pièce d'identité.

Données à caractère personnel - toute information concernant une personne physique identifiée ou identifiable. Une "personne physique identifiable" est une personne qui peut être identifiée,

directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

Données biométriques - données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique.

Données supplémentaires - données acquises par le service de vérification d'identité à distance et transmises au service commercial dans le cadre du résultat de la vérification d'identité à distance, mais sur lesquelles aucune vérification n'est effectuée par le service dans le cadre du référentiel. Les données supplémentaires ne sont pas incluses dans le résultat de la vérification d'identité à distance. L'acquisition par le service de vérification d'identité à distance de ces données supplémentaires et leur transmission au service commercial doivent être conformes à la réglementation applicable et sont généralement demandées par le client pour répondre aux exigences réglementaires.

Preuve de vérification de l'identité - enregistrement, par le prestataire de services, des informations pertinentes à produire à des fins de résolution des litiges ou d'enquête, et pour fournir des preuves devant les tribunaux. Cette norme précise les données minimales à conserver. Les données contenues dans le dossier de preuve ne sont pas conservées pour le traitement biométrique.

État de l'art - ensemble des meilleures pratiques, technologies et documents de référence accessibles au public en matière de sécurité des systèmes d'information ou de vérification de l'identité, ainsi que les informations qui en découlent clairement. Ces documents peuvent être publiés sur l'internet par la communauté de la sécurité des systèmes d'information, diffusés par des organisations de référence, ou être d'origine législative, réglementaire ou normative.

Détenteur légitime du document d'identité - la personne à qui le document d'identité a été délivré par le pays émetteur et dont l'identité est représentée par ce document d'identité.

Raison de l'échec - la cause de l'échec de la vérification d'identité à distance. La raison de l'échec est communiquée par le service de vérification d'identité à distance à l'unité opérationnelle ou à l'utilisateur et est utilisée pour faire la distinction entre un échec dû à une suspicion de fraude et un échec dû à des raisons techniques (résolution insuffisante de la caméra du terminal, luminosité insuffisante, problème de mise au point, etc.) Dans le cas d'une suspicion de fraude, le motif ne comporte aucune information sur les contrôles effectués ou sur le type de fraude suspectée.

Moyen d'identification électronique - élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.

Niveau d'assurance élevé - ce niveau est destiné à prévenir le risque d'usurpation ou d'altération d'identité. Un service de vérification d'identité à distance est dit de niveau d'assurance élevé lorsqu'il est démontré qu'il répond aux exigences du référentiel pour le niveau élevé.

Niveau d'assurance substantiel - ce niveau est destiné à réduire substantiellement le risque d'usurpation ou d'altération d'identité. Un service de vérification d'identité à distance est considéré comme ayant un niveau d'assurance substantiel lorsqu'il est démontré qu'il répond aux exigences de la norme pour le niveau substantiel.

Opérateur - personnel du service de vérification d'identité à distance chargé de vérifier l'identité des utilisateurs, de prononcer le verdict de réussite ou d'échec de la vérification d'identité à distance et d'alerter un spécialiste de la fraude en cas de suspicion d'usurpation d'identité.

Politique de vérification de l'identité à distance - ensemble de règles, référencées de manière unique par un OID, définissant les exigences auxquelles un prestataire de services de vérification de l'identité à distance se conforme dans la mise en place et la fourniture de son service. Une politique de vérification de l'identité à distance peut également, si nécessaire, définir des obligations et des exigences à l'égard d'autres parties prenantes, y compris les Utilisateurs et les clients. La politique de vérification de l'identité à distance est mise à la disposition des utilisateurs.

Potentiel d'attaque - mesure de l'effort nécessaire pour attaquer un service de vérification d'identité à distance, exprimée en termes d'expertise, de ressources et de motivation d'un attaquant. L'annexe B.4 du [CC_CEM] donne des indications sur le calcul d'un potentiel d'attaque élevé ou modéré.

Prestataire - une entité juridique qui fournit un service de vérification d'identité à distance. IDnow est le Prestataire.

Service - la fourniture du service de vérification d'identité à distance à un client, dans le cadre de l'accord de service entre le fournisseur et le client.

Spécialiste de la fraude à l'identité - personnel du service de vérification d'identité à distance ayant une connaissance approfondie des caractéristiques de sécurité des documents d'identité et une expertise dans la détection de la fraude à l'identité.

Spécialiste de la fraude biométrique - personnel du service de vérification d'identité à distance ayant une connaissance approfondie de la biométrie et une expertise dans la détection de la fraude biométrique.

Résultat de la vérification d'identité à distance (RVID) - ensemble d'informations transmises par le service de vérification d'identité à distance au service métier, comprenant le verdict (succès ou échec) de la vérification d'identité à distance, la raison de l'échec, le cas échéant, les attributs de l'identité de l'utilisateur requis par le service métier et vérifiés par le Prestataire, ainsi que toute donnée supplémentaire requise par le service métier.

Sous-traitance - processus par lequel le prestataire de services sous-traite tout ou partie de l'exécution de l'accord de service (et du contrat, le cas échéant) avec le client.

Service de vérification d'identité à distance - service couvert par la présente norme, chargé d'acquérir et de vérifier les informations d'identification des utilisateurs, de constituer le dossier de preuve et de transmettre le résultat de la vérification d'identité à distance au service commercial.

Service de vérification d'identité à distance asynchrone - un service de vérification d'identité à distance est dit asynchrone lorsque la phase de vérification des données d'identification est effectuée après la phase d'acquisition des données d'identification.

Service de vérification d'identité à distance externe - un service de vérification d'identité à distance est dit externe s'il ne répond pas aux critères d'un service interne.

Service hybride de vérification d'identité à distance - un service de vérification d'identité à distance est dit hybride si le résultat de la vérification d'identité à distance ne peut être déclaré "réussi" par un opérateur qu'après que celui-ci a validé les résultats des vérifications effectuées par des processus automatisés et procédé à sa propre vérification des données d'identification.

Service de vérification d'identité à distance synchrone - un service de vérification d'identité à distance est dit synchrone lorsqu'il ne répond pas aux critères d'un service de vérification d'identité à distance asynchrone.

Service de vérification d'identité à distance synchrone avec interaction humaine - un service de vérification d'identité à distance est dit synchrone avec interaction humaine lorsqu'il est synchrone et permet des interactions entre l'utilisateur et l'opérateur pendant l'acquisition ou la vérification des données d'identification. Un service de vérification d'identité à distance synchrone avec interaction humaine peut, par exemple, permettre à un opérateur de guider l'utilisateur pendant l'acquisition des données d'identification.

Service de vérification d'identité à distance synchrone sans interaction humaine - un service de vérification d'identité à distance est dit synchrone sans interaction humaine lorsqu'il est synchrone et ne permet aucune interaction entre l'utilisateur et l'opérateur pendant l'acquisition et la vérification des données d'identification. Le service peut toutefois mettre en œuvre des interactions automatisées avec l'utilisateur.

Service commercial - le service auquel l'utilisateur souhaite s'identifier, sous la responsabilité du client, en utilisant le service de vérification d'identité à distance.

Terminal - le matériel (téléphone mobile, tablette, ordinateur, etc.) utilisé pour acquérir les données d'identification de l'utilisateur. Le terminal peut être celui de l'utilisateur, du fournisseur ou du client. L'acquisition des données d'identification de l'utilisateur via le terminal peut être réalisée à l'aide de tous types d'applications : application mobile dédiée, navigateur, etc.

Traitement - toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Document d'identité - document officiel certifiant l'identité d'une personne. Les documents d'identité visés à l'annexe 2 de la présente PVID sont acceptés dans le cadre de la présente PVID.

Utilisateur - personne physique dont l'identité est vérifiée par le service de vérification d'identité à distance.

L'usurpation d'identité est le fait d'utiliser frauduleusement les données d'identification d'un tiers. Dans le contexte de la présente norme, la notion d'usurpation d'identité englobe également l'altération de l'identité, qui consiste à utiliser des données d'identification frauduleuses n'appartenant pas à une personne existante.

Verdict de vérification d'identité à distance - verdict binaire ("réussite" ou "échec") généré par le service de vérification d'identité à distance après les phases d'acquisition et de vérification des données d'identification. Le verdict est "réussite" si le service de vérification d'identité à distance conclut que la pièce d'identité présentée par l'utilisateur est authentique, d'une part, et que l'utilisateur est le détenteur légitime de la pièce d'identité, d'autre part ; dans le cas contraire, le verdict est "échec".

2. PROCESSUS DE VÉRIFICATION DE L'IDENTITÉ À DISTANCE

2.1 LANGUE DU SERVICE

Les opérateurs parlent les langues suivantes :

- Français
- Anglais
- Allemand

L'interface utilisateur est disponible dans les langues suivantes :

- Français
- Anglais
- Allemand

Il est précisé que la langue française est disponible aux horaires suivants : 8:00 - 22:00, 7 jours par semaine.

Avant d'utiliser le service, l'utilisateur est invité à choisir sa langue. La sélection de la langue peut se faire soit directement dans l'interface utilisateur, soit en changeant la langue de l'appareil.

Tous les opérateurs d'IDnow sont situés dans des pays membres de l'UE. Les pays sont communiqués à l'ouverture du service PVID et sélectionné par l'Utilisateur.

2.2 TERMINAL

Le terminal utilisé pour le service est le téléphone portable ou l'ordinateur de l'Utilisateur.

Si le terminal est un téléphone mobile, l'application est soit fournie par IDnow (par exemple, l'application " IDnow Online-Ident "), soit fournie par le client lorsque la technologie d'IDnow est intégrée à l'aide d'un SDK. Ces applications sont disponibles dans le magasin de confiance autorisé du fournisseur de téléphone portable (par exemple, Apple, Google). IDnow surveille les magasins d'applications officiels pour détecter la disponibilité d'applications frauduleuses conçues pour remplacer l'application légitime du service.

Cette application, quel que soit le terminal, n'est pas utilisée pour aider au calcul du verdict du VID ou effectuer un contrôle technique utilisé dans l'opération de VID. Cette application ne sert qu'à prendre le contrôle de la caméra sur le téléphone portable.

La caméra du terminal doit pouvoir avoir une résolution minimale au moins égale à 720p : 1280 × 720 à 25 images par seconde après compression de la vidéo de la pièce d'identité et du visage de l'Utilisateur pour permettre au service PVID d'effectuer les vérifications.

2.3 DOCUMENT D'IDENTITÉ

La politique de vérification d'identité à distance n'est mise à jour sur les questions relatives aux documents d'identité qu'après validation formelle par un spécialiste de la fraude à l'identité.

Seuls les documents d'identité conformes aux règles définies à l'annexe 1 sont autorisés à être utilisés dans le cadre du service certifié. Les nouveaux documents sont approuvés après validation par l'ANSSI via le processus de rapport de changement.

Tous les documents d'identité utilisés par IDnow dans le cadre du service sont supervisés par un spécialiste de la fraude de l'équipe de gestion de la qualité.

Seule une pièce d'identité non périmée peut être utilisée dans le cadre du service VID.

Lorsqu'il est disponible et légalement autorisé, IDnow utilise le service de contrôle des documents d'identité pour vérifier la validité du document d'identité fourni par le pays qui a délivré le document d'identité utilisé par l'Utilisateur pour une opération de VID. Si le service renvoie un résultat non valide pour un document d'identité, le résultat renverra toujours le résultat « échec ».

IDnow vérifie si le document d'identité présente des altérations physiques (document d'identité déchiré ou rayé, etc.), comme décrit dans la DPVID.

IDnow a pris des mesures supplémentaires pour aider les Utilisateurs handicapés, notamment en garantissant un contraste élevé. En raison de la nature du processus (enregistrement vidéo), il existe certaines limitations concernant les handicapés qui peuvent exécuter le processus avec succès (par exemple, les utilisateurs aveugles).

Le numéro du passeport ou de la pièce d'identité est vérifié par rapport à la norme OACI et au PRADO. Si un contrôle de validité du document d'identité est effectué et qu'il conclut que le document d'identité n'est pas valide, le verdict du VID est toujours "échec".

Le service VID acquiert une vidéo du document d'identité.

Lors de l'obtention de la pièce d'identité de l'Utilisateur, il lui sera demandé :

- L'Utilisateur interagisse avec un opérateur par vidéo pendant toute la durée de la session.
- Prendre une photo du recto du document
- Prendre une photo du verso du document
- Inclinez le document pour faire apparaître les éléments de sécurité.
- Suivre les instructions de l'opérateur concernant la qualité des images (document non net, reflets couvrant le document, doigts sur le document, luminosité insuffisante).

2.4 CORRESPONDANCE DES VISAGES ET DÉTECTION DE LA PHYSIONOMIE

La présente politique de vérification d'identité à distance n'est mise à jour sur des sujets liés à la biométrie qu'après validation formelle par un spécialiste de la fraude biométrique et validation par l'ANSSI au travers du processus de déclaration de changement.

IDnow a pris des mesures supplémentaires pour aider les utilisateurs handicapés, notamment en garantissant un contraste élevé. En raison de la nature du processus (enregistrement vidéo), il existe certaines limitations concernant les handicaps qui peuvent exécuter le processus avec succès (par exemple, les utilisateurs aveugles).

Le service VID acquiert une vidéo du visage de l'Utilisateur.

Lors de l'acquisition du visage de l'Utilisateur, il lui sera demandé de

- D'interagir avec un opérateur par vidéo pendant toute la durée de la session.
- Prendre une photo de son visage ("Selfie")
- Effectuer des mouvements en fonction des instructions de l'opérateur ("Liveness Detection")
- Suivre les instructions de l'opérateur concernant la qualité des images (visage mal cadré, pas assez lumineux).

Il est garanti qu'aucun traitement biométrique n'est conservé plus de 96 heures.

2.5 VÉRIFICATION INITIALE DE L'IDENTITÉ À DISTANCE

2.5.1 PROCESSUS DE VID

Dans tous les cas, l'Utilisateur doit disposer d'un Terminal, d'une pièce d'identité et être capable de parler la langue comprise par l'Opérateur. Si l'Utilisateur ne peut pas utiliser le service VID pour une raison quelconque, distincte de celle énumérée aux paragraphes 2.3 et 2.4 ci-dessus, il incombe à l'Utilisateur de fournir une solution alternative au service de VID.

L'Utilisateur doit présenter une pièce d'identité valide et son visage pour que le service puisse l'identifier (voir les points 2.3 et 2.4 ci-dessus).

Une fois l'acquisition effectuée, l'Opérateur vérifie les données d'identification, le visage de l'Utilisateur par rapport au visage contenu dans la pièce d'identité, la validité du visage de l'Utilisateur et l'authenticité de la pièce d'identité, et rend un verdict ou un rapport intermédiaire en cas d'avis contradictoire avec le contrôle automatique. En cas de rapport intermédiaire, l'Opérateur demande au spécialiste de la fraude à l'identité et/ou au spécialiste de la fraude biométrique, en fonction du point à vérifier et/ou de la contradiction avec les contrôles automatiques, de prendre une décision.

Il y a toujours un deuxième opérateur qui vérifie les contrôles effectués par l'opérateur initial. C'est le deuxième opérateur qui donne le verdict final.

2.5.2 INFORMATIONS NON VÉRIFIÉES SUR LES UTILISATEURS

IDnow n'utilise aucune information non vérifiée dans les services VID. Les attributs d'identité sont vérifiés par rapport au document d'identité et les données supplémentaires sont au moins collectées pendant la session VID afin qu'IDnow puisse confirmer qu'elles sont réclamées par l'Utilisateur.

2.5.3 VALIDATION DE L'AUTORITÉ

IDnow n'accepte que les personnes physiques telles qu'elles sont identifiées dans un document d'identification et ne vérifie pas d'autres attributs de l'utilisateur.

2.5.4 VERDICT DU VID

Le verdict du VID donné par le service est automatiquement "échec", sans intervention d'un opérateur, si le traitement automatisé relatif à la vérification de l'authenticité du document d'identité conclut que le document d'identité n'est pas authentique.

2.6 IDENTITÉ DE L'UTILISATEUR

Dans le cadre du service VID, le nom de l'Utilisateur est comparé à une extraite de la pièce d'identité.

IDnow collecte les données de l'utilisateur et les vérifie. Les données suivantes seront collectées à minima et si elles sont applicables au Client :

- Attribut d'identité :
  - Nom complet
  - Lieu de naissance
  - Date de naissance
  - Nationalité
  - Numéro de la carte d'identité
  - Pays d'émission
  - Type de document d'identité
  - Date d'émission
  - Date de validité
  - Une photographie du visage de l'Utilisateur extraite de la vidéo du visage de l'Utilisateur
  - Une photographie de la pièce d'identité extraite de la vidéo de la pièce d'identité de l'Utilisateur

- Données supplémentaires (facultatives) :
  - Numéro de téléphone mobile
  - Adresse électronique de l'Utilisateur
  - Informations sur l'Opérateur chargé de l'identification
  - Information sur la date de l'identification
  - La vidéo du visage de l'Utilisateur
  - La vidéo de la pièce d'identité de l'Utilisateur

Les détails se trouvent dans le document "IDnow VideoIdent Qualified Electronic Signature Process Description", section 3.4.

Les données supplémentaires ne sont pas prises en compte dans le processus de conclusion du verdict de la PVID.

2.6.1. ANONYMAT OU PSEUDONYMAT

Tous les noms sont des noms réels et ont été vérifiés à l'aide d'une pièce d'identité. L'anonymat ou le pseudonymat ne seront pas acceptés par IDnow.

2.6.2. RÈGLES D'INTERPRÉTATION DE L'IDENTITÉ EN RVID

L'identité contenue dans le RVID sera toujours tirée du document d'identité utilisé pour identifier l'Utilisateur.

2.6.3. UNICITÉ DE L'IDENTITÉ

L'unicité de l'identité de chaque Utilisateur est garantie en fournissant le nom complet de l'Utilisateur associé au type de document d'identité et au numéro de série du document d'identité utilisé par l'Utilisateur pour être identifié.

2.7 RÉSULTAT DE LA VÉRIFICATION DE L'IDENTITÉ À DISTANCE (RVID)

2.7.1 CREATION

Chaque fois qu'un Opérateur a décidé d'un verdict (succès ou échec) pour une VID concernant un Utilisateur, IDnow génère un RVID unique associé à cet Utilisateur.

Le résultat du VID est uniquement composé du verdict (succès ou échec) de la vérification et des attributs d'identité de l'Utilisateur (voir le point 2.6 ci-dessus), ainsi que toute donnée supplémentaire demandée par le service commercial du Client. Le RVID ne contient que l'attribut d'identité de l'Utilisateur tel que défini au point 2.6 ci-dessus.

Le RVID ne contient aucun élément relatif aux résultats des contrôles effectués par le service autre que le verdict (succès ou échec) et notamment aucune note calculée sur la base de ces contrôles.

Il est interdit à l'Utilisateur de corriger ou de supprimer le dossier de preuve et le RVID transmis au Client, ainsi que toutes les informations nécessaires à l'établissement du résultat. Il lui est également interdit d'accéder aux données ayant fait l'objet d'un traitement automatisé ou manuel.

2.7.2 STOCKAGE

Le RVID est stocké de la même manière que la preuve VID au même endroit.

2.7.3 TRANSMISSION

Quel que soit le résultat du verdict (succès ou échec), le RVID est transmis au Client.

Le RVID est transmis au Client par le biais d'une communication TLS.

Le délai maximum entre le début de l'acquisition des données d'identification de l'Utilisateur et la transmission du RVID au Client ne peut excéder 96 heures.

2.8 PREUVE DE VÉRIFICATION D'IDENTITÉ À DISTANCE

Pour chaque opération VID, quel que soit le verdict donné par l'Opérateur, IDnow génère une preuve VID unique.

La preuve VID contient au minimum les données suivantes :

- Données d'identification :
  - Vidéo d'un document d'identité capturé au cours de la procédure VID.
  - Vidéo du visage de l'abonné capturée au cours du processus de VID.
- Date et heure de la capture de la vidéo du document d'identité.

- Date et heure de la capture de la vidéo du visage de l'Utilisateur.
- La liste de tous les contrôles effectués sur les données d'identification, et pour chaque contrôle :
    - Date et heure du contrôle.
    - Opération associée au contrôle, y compris :
        - Vérification de l'authenticité du document d'identité.
        - Détection de la vivacité du visage de l'Utilisateur.
        - Comparaison du visage de l'Utilisateur avec le visage contenu dans le document d'identité.
    - Le type de contrôle : automatique ou manuel.
    - L'identité de l'Opérateur ou du spécialiste de la fraude (spécialiste de la fraude à l'identité et/ou spécialiste de la fraude biométrique) qui a effectué le contrôle lorsque celui-ci est manuel.
    - Le pays à partir duquel l'Opérateur ou le spécialiste de la fraude (spécialiste de la fraude à l'identité et/ou spécialiste de la fraude biométrique) a effectué le contrôle lorsqu'il est manuel.
    - La version et la configuration, le cas échéant, des outils qui ont effectué le contrôle lorsqu'il est automatique. Cela peut se faire en stockant l'horodatage de l'identification et en stockant la version et la configuration de l'outil qui était actif à ce moment-là.
    - Les rapports intermédiaires émis par le traitement automatisé, l'Opérateur ou le spécialiste de la fraude (spécialiste de la fraude à l'identité et/ou spécialiste de la fraude biométrique) à la suite du contrôle.
- Le verdict de la vérification de l'identité à distance (succès ou échec).
- Les raisons données par l'Opérateur en cas de verdict "échec".
- L'identité de l'Opérateur qui a rendu le verdict.
- La date à laquelle l'Opérateur a rendu le verdict.
- Le pays à partir duquel l'Opérateur a rendu le verdict.
- Le nom complet de l'Utilisateur tel qu'il figure dans le document d'identité.
- La date et le lieu de naissance de l'Utilisateur.
- Numéro unique du document d'identité.
- La date de délivrance du document d'identité.
- La date d'expiration du document d'identité.
- Le résultat du VID transmis au Client.

La preuve VID ne contient pas de données relatives au traitement biométrique.

Par défaut, la preuve du VID n'est pas transmise au Client. Seuls les Clients allemands couverts par la loi allemande "Geldwäschegesetz", "Vertrauensdienstegesetz" ou la "Telekommunikationsgesetz" peuvent recevoir la copie de la preuve VID qui comprend la vidéo de la pièce d'identité capturée pendant le processus VID et la vidéo du visage de l'Utilisateur capturée pendant le processus VID.

2.9 CHANGEMENT D'IDENTITE

Si l'Utilisateur change d'identité, le RVID actuellement utilisé n'est plus valide. Dans ce cas, l'Utilisateur doit refaire un nouveau VID pour créer un nouveau RVID si le Client a besoin d'un RVID pour cet Utilisateur.

2.10 FRAUDES

IDnow génère une alerte pour chaque vol d'identité suspecté ou réel, qu'il soit détecté par le prestataire de services ou signalé par le client.

Les réclamations dont dispose l'Utilisateur du service, notamment aux fins d'annulation d'une identification frauduleuse ou en cas de refus d'identification d'un utilisateur de bonne foi, peuvent être adressées directement à support@mail.idnow.de.

IDnow définit des indicateurs pour détecter les tentatives d'usurpation d'identité liées aux scénarios de risque identifiés dans l'évaluation des risques d'usurpation d'identité.

2.11 BULLETINS OPÉRATIONNELS

IDnow établit des bulletins opérationnels et inclut, depuis le dernier bulletin opérationnel, au moins les éléments suivants :

- Les indicateurs opérationnels du service (voir section 2.12).
- Un examen des plaintes reçues, en cours et clôturées.
- Un examen des incidents de sécurité liés à la sécurité des systèmes informatiques.
- Une revue des incidents de sécurité notifiés à l'ANSSI.
- Date de la dernière exécution du plan de test concernant la capacité effective du service VID à détecter les tentatives d'usurpation d'identité.
- Le taux de faux négatifs (FNR) et le taux de faux positifs (FPR) pour la vérification de l'authenticité de la pièce d'identité, mesurés lors de la dernière exécution du plan d'essai de la capacité effective du service à détecter les tentatives d'usurpation d'identité.
- Le taux de faux négatifs (FNR) et le taux de faux positifs (FPR) pour la comparaison du visage de l'Utilisateur mesuré lors de la dernière exécution du plan de test de la capacité effective du service à détecter les tentatives d'usurpation d'identité.
- Le taux de faux négatifs (FNR) et le taux de faux positifs (FPR) pour la détection en direct, mesurés lors de la dernière exécution du plan de test, de la capacité effective du service à détecter les tentatives d'usurpation d'identité.
- Un examen de tous les changements apportés à :
    - Le système d'information du service VID.
    - à l'évaluation des risques liés à l'usurpation d'identité, en particulier si la liste des scénarios de risque a été modifiée.
    - L'évaluation des risques liés à la sécurité des systèmes d'information, en particulier si la liste des scénarios de risque a été modifiée.
    - Le plan de traitement des risques.
    - La politique VID.
    - La déclaration de pratique de la VID.

- La politique de sécurité d'IDnow
- Le plan d'essai pour tester la capacité effective du service à détecter les tentatives d'usurpation d'identité.

IDnow transmet au Client, à la fréquence définie dans le Contrat avec le Client, les bulletins opérationnels relatifs au service de vérification d'identité à distance.

IDnow assure la confidentialité des bulletins opérationnels.

2.12 CONTRAT DE SERVICE VID ET SLA

IDnow et le client doivent établir un contrat pour permettre au client d'utiliser le service VID qui contient les informations requises définies dans le référentiel PVID (§ IV.7.2 de la présente norme).

Le contrat décrit :

- l'organisation, la portée et les objectifs du service de vérification d'identité à distance, ainsi que les moyens techniques et organisationnels.
- les modalités de mise à jour de la politique de vérification d'identité à distance et, le cas échéant, les modalités de validation de ces modifications par le Client.
- si l'accès à distance est autorisé.
- que cette politique soit annexée au contrat.
- un point de contact pour le client.
- le lieu de traitement et de stockage des données du service de vérification de l'identité à distance pour ce client, y compris les données de l'utilisateur.
- qu'IDnow doit notifier au client toute rupture du contrat.
- qu'IDnow notifiera le Client en cas d'incident de sécurité détecté sur le système d'information du Service de Vérification d'Identité à Distance.
- les modalités et le délai maximum de transmission au client des informations relatives à l'incident de sécurité.
- qu'IDnow n'effectue que des actions strictement conformes aux objectifs du service.
- que le client doit déposer une plainte pour tous les contrôles d'identité à distance pour lesquels le prestataire de services a prononcé un verdict de "réussite" et pour lesquels le client soupçonne ou a détecté une usurpation d'identité.
- Que le Client remplisse toutes les obligations légales nécessaires au service et celles relatives à la collecte, au traitement et au transfert de données à caractère personnel et au traitement biométrique. Le contrat doit préciser les finalités de cette collecte, de ce traitement et de ce transfert et identifier le cadre réglementaire applicable.
- les responsabilités et les mesures prises respectivement par IDnow et le client pour réduire les risques potentiels liés au service, ceux relatifs à l'usurpation d'identité et à la collecte et au traitement de données à caractère personnel.
- qu'IDnow dispose d'une assurance professionnelle couvrant tout dommage causé au service commercial et à son système d'information dans le cadre de la fourniture du service, préciser la couverture de l'assurance et inclure le certificat d'assurance.
- les mesures mises en œuvre par IDnow dans le cadre de son plan de cessation d'activité.
- qu'IDnow ne collecte et ne traite que des données adéquates, pertinentes et limitées à ce qui est nécessaire aux fins pour lesquelles elles sont traitées.

- qu'IDnow ne divulgue aucune donnée utilisateur à des tiers, sauf avec le consentement écrit exprès du client et conformément au RGPD.
- les clauses relatives à l'éthique d'IDnow et comprennent le code de conduite d'IDnow.
- les modalités d'accès, de stockage, de transport, de reproduction, de destruction et de restitution des données relatives à ce sponsor, notamment celles relatives aux utilisateurs.
- que seule la version française fait foi, notamment en cas de litige.
- les moyens techniques et organisationnels mis en œuvre par IDnow pour assurer le respect des lois et réglementations applicables, celles relatives au RGPD.
- les exigences légales et réglementaires spécifiques auxquelles le client est soumis, celles liées à son secteur d'activité.
- que la législation applicable au contrat est la loi française.
- qu'IDnow peut, si nécessaire, sous-traiter tout ou partie du service à un autre prestataire, ci-après dénommé le " sous-traitant ", pour autant que toutes les conditions énoncées ci-dessous soient remplies :
    - il existe un contrat de service entre IDnow et le sous-traitant ;
    - le recours à la sous-traitance est connu et formellement accepté par écrit par le client ;
    - le sous-traitant se conforme aux exigences de ces normes.
- les livrables attendus dans le cadre du service, les règles de propriété et les niveaux de sensibilité relatifs à ces livrables, ainsi que les conditions de protection associées.
- que les livrables du service sont en langue française, sauf demande écrite formelle du client.
- des indicateurs opérationnels pour mesurer le niveau de service fourni.
- la fréquence à laquelle IDnow transmet des bulletins opérationnels au client.
- qu'IDnow définisse et mette en œuvre un processus d'amélioration continue de l'efficacité du service de vérification d'identité à distance basé notamment sur des indicateurs opérationnels.
- identifier les créneaux horaires opérationnels pour le service de vérification d'identité à distance.
- que le service doit procéder à une authentification mutuelle avec le service commercial lorsqu'il lui transmet des résultats, et garantir l'intégrité, la confidentialité et l'impossibilité de rejouer les données transmises.

IDnow ne fournira aucun service tant que le contrat n'aura pas été formellement approuvé par écrit par le client. Le contrat est rédigé en français. Une traduction de courtoisie du contrat est fournie à la demande du client.

IDnow développe et met en œuvre un processus de capitalisation des incidents et fraudes détectés afin d'améliorer continuellement l'efficacité de son service VID. IDnow définit avec le client les indicateurs opérationnels du service VID. IDnow développe et maintient un processus de mesure des indicateurs décrivant, pour chacun des indicateurs opérationnels définis pour le Client, les méthodes et moyens utilisés pour mesurer l'indicateur.

Au minimum, IDnow met en place les moyens de mesurer les indicateurs opérationnels suivants :

- Le temps d'attente moyen, minimum et maximum pour les utilisateurs.
- Nombre de contrôles d'identité à distance effectués.
- Nombre de contrôles d'identité à distance par verdict (succès ou échec).

- Nombre de contrôles d'identité à distance pour lesquels le service a émis un verdict d'échec, en fonction de la raison de l'échec.
- Nombre de contrôles d'identité à distance pour lesquels le service a rendu un verdict d'échec au motif que l'usurpation d'identité était suspectée ou avérée, selon la nature de la tentative d'usurpation d'identité.
- Le nombre de contrôles d'identité à distance pour lesquels le service a émis un verdict de "succès" et qui se sont révélés être une usurpation d'identité après coup, selon que l'usurpation d'identité a été détectée par le prestataire de services ou par le client.
- Nombre de demandes d'indemnisation reçues, en cours de traitement ou clôturées.
- Le délai moyen, minimum et maximum de clôture des sinistres.

3. INSTALLATIONS, GESTION ET CONTRÔLES OPÉRATIONNELS

3.1. CONTRÔLES PHYSIQUES

Des contrôles physiques ont été mis en place pour les sites utilisés pour traiter et stocker les données personnelles du processus d'inscription afin d'empêcher tout accès non autorisé à ces installations : Le centre d'identification et le centre de données.

IDnow établit et tient à jour une liste des personnes autorisées à accéder aux locaux hébergeant le système d'information du service VID. IDnow met en place des mécanismes de journalisation des accès aux locaux hébergeant le système d'information du service VID.

IDnow définit et met en œuvre des mesures pour assurer la confidentialité et l'intégrité des journaux d'accès aux locaux hébergeant le service VID.

Les mesures suivantes (voir la politique d'infrastructure du centre d'identification IDnow, chapitre 3) ont été mises en œuvre pour le centre d'identification :

- Fenêtres et portes fermées
- Restriction de l'accès physique, authentification uniquement par puce + pin
- Registres d'accès par porte au centre d'identification
- Vidéosurveillance
- Supervision ou contrôle de tiers
- Contrôle de l'accès au centre d'identification

En outre, IDnow utilise plusieurs centres d'identification distincts afin de minimiser l'impact de l'exposition à l'eau et au feu. Aucune donnée n'est stockée de manière permanente dans les centres d'identification.

IDnow fait appel à un sous-traitant pour l'exploitation du centre de données. Il fournit le matériel, les racks, la connexion au réseau, l'électricité et le contrôle climatique pour l'exploitation des serveurs. IDnow prend en charge l'exploitation, y compris le niveau du système d'exploitation.

Les mesures suivantes (voir la politique d'infrastructure du centre de données, chapitre 3) ont été mises en œuvre pour le centre de données :

- Fenêtres et portes fermées
- Contrôle de l'eau et de l'incendie
- Connexions / alimentations redondantes
- Registres d'accès aux portes
- Système d'alarme de danger
- Vidéosurveillance
- Protection du périmètre / cabines de porteurs
- Supervision ou contrôle de tiers
- Contrôle de l'accès au centre de données
- Visites de contrôle
- Destruction/élimination sécurisée

En outre, toutes les données du centre de données sont sauvegardées sur un site extérieur.

IDnow dispose d'un système de gestion et de classification des actifs dans lequel tous les systèmes pertinents sont enregistrés et classés en fonction du niveau de sécurité requis. Le responsable de la sécurité informatique en est chargé et vérifie la gestion des actifs deux fois par an.

On s'assure que les contrôles physiques sont en place pour protéger les actifs conformément à leur classification.

3.2. CONTRÔLES PROCÉDURAUX

IDnow a mis en œuvre un concept de rôle qui garantit que les tâches pertinentes sont séparées de manière à assurer des contrôles efficaces. Le personnel occupant un rôle de confiance est nommé et accepté par la direction. La personne chargée de remplir le rôle doit également l'accepter. Les preuves sont documentées en conséquence. Pour chaque rôle de confiance, les responsabilités sont définies dans les descriptions de poste respectives. L'accès aux données n'est accordé aux employés ayant les rôles respectifs qu'après les vérifications nécessaires. Ces droits ne sont accordés que si le rôle spécifique a été assigné à une tâche qui nécessite un tel accès aux données, conformément au principe du "moindre privilège".

Une séparation des tâches conflictuelles et des domaines de responsabilité est mise en œuvre.

Les détails se trouvent au chapitre 5 "Concept de rôle" de la "Politique de sécurité d'IDnow".

3.3. CONTRÔLE DU PERSONNEL

IDnow s'assure que les agents chargés du processus d'inscription possèdent les qualifications et les compétences nécessaires. Pour ce faire, une formation de plusieurs jours est organisée après le recrutement et avant le déploiement dans les opérations de production. IDnow fournit un plan de formation détaillé dans lequel toutes les formations initiales et récurrentes sont énumérées. Le plan de formation comprend également une formation sur les nouvelles menaces et les pratiques de sécurité actuelles, qui a lieu au moins tous les 12 mois. La documentation relative à la formation est conservée dans le système de gestion des ressources humaines et dans un coffre-fort ignifugé. La responsabilité de l'exécution de la formation incombe au chef d'équipe du centre d'identification et au directeur des ressources humaines.

La fiabilité de l'employé est déterminée par IDnow en exigeant tous les documents pertinents (en particulier le certificat de police, les informations sur la solvabilité et le CV) de cet employé. Lors de l'examen du certificat de police, chaque entrée de l'employé dans le certificat doit être vérifiée séparément par le responsable des ressources humaines et le responsable de la sécurité informatique, puis approuvée ou rejetée et, si aucune entrée ne doit exister, aucune autorisation distincte n'est requise. Si un pays ne dispose pas de l'un des mécanismes énumérés ci-dessus (par exemple, pas d'informations sur la solvabilité), IDnow doit utiliser d'autres mesures offrant un niveau d'assurance équivalent quant à la fiabilité de l'employé. Ces contrôles doivent être effectués avant le recrutement et révisés régulièrement (la période entre deux révisions ne doit pas dépasser trois ans). Les opérateurs et les spécialistes de la fraude doivent être liés contractuellement à IDnow.

IDnow, après le recrutement, sensibilise les opérateurs et les spécialistes de la fraude aux risques spécifiques liés à leur fonction, et les informe de leur obligation de discrétion.

IDnow emploie un nombre suffisant d'opérateurs et de spécialistes de la fraude effectuant les tâches et disposant des compétences identifiées dans l'annexe 2 de la norme PVID de l'ANSSI pour réaliser pleinement tous les aspects du service VID.

IDnow fournit aux Opérateurs et aux spécialistes de la fraude tout le matériel pédagogique et technique leur permettant de mener à bien les missions qui leur sont confiées.

IDnow élabore et met en œuvre un plan de formation régulier pour les opérateurs et les spécialistes de la fraude conformément aux missions et compétences identifiées dans l'annexe 2 de la norme PVID de l'ANSSI.

IDnow développe et met en œuvre un plan de contrôle régulier pour vérifier que les opérateurs et les spécialistes de la fraude possèdent les compétences identifiées dans l'annexe 2 de la norme PVID de l'ANSSI.

IDnow s'assure que chaque opérateur et spécialiste de la fraude, avant l'exécution du service, a suivi le plan de formation et passé le plan de contrôle.

IDnow s'assure que toutes les personnes jouant un rôle de confiance dans les opérations de l'AR sont libres de tout conflit d'intérêts susceptible de nuire à l'impartialité des opérations. Le directeur des ressources humaines est responsable des sanctions disciplinaires (pouvant aller jusqu'à la résiliation du contrat) si le personnel enfreint les politiques ou les procédures d'IDnow. C'est également le cas pour les employés des tiers auxquels IDnow fait appel pour l'externalisation. Les employés jouant un rôle de confiance auprès de ces parties doivent satisfaire aux mêmes exigences que les employés internes en ce qui concerne la fiabilité.

IDnow utilise un processus d'examen pour détecter les identifications incorrectes et vérifier si les politiques et procédures d'identification ont été respectées. En outre, IDnow procède à des tests d'identification à des fins de contrôle de la qualité. L'objectif de ces tests d'identification est de vérifier que toutes les procédures sont respectées. Ces tests d'identification sont effectués au moins une fois par an. Le responsable est le chef d'équipe du centre d'identification.

Les détails concernant les contrôles personnels peuvent être trouvés dans la "Politique RH d'IDnow".

3.3.1 EXIGENCES RELATIVES AUX ENTREPRENEURS INDÉPENDANTS

IDnow fait appel à un sous-fournisseur pour l'hébergement du matériel serveur. Il fournit le matériel, les racks, la connexion au réseau, l'électricité et le contrôle climatique pour le fonctionnement des serveurs. IDnow prend en charge l'exploitation, y compris le niveau du système d'exploitation.

IDnow stocke elle-même les fichiers d'épreuves VID ou fait appel à un sous-traitant pour l'archivage à long terme des fichiers d'épreuves VID.

IDnow utilise à la fois des centres d'identification internes et des sous-fournisseurs pour les centres d'identification externes.

3.3.2. DOCUMENTATION FOURNIE AU PERSONNEL

IDnow met à la disposition de son personnel la présente politique de vérification d'identité à distance et la DPVID, ainsi que toutes les procédures et politiques pertinentes. D'autres documents techniques, opérationnels et administratifs (par exemple, le manuel de l'administrateur, le manuel de l'utilisateur, etc.) sont fournis pour permettre au personnel d'exercer ses fonctions.

3.3.3 CODE D'ÉTHIQUE

IDnow dispose d'un code de déontologie qui est intégré au règlement intérieur et qui stipule notamment que :

- Les services sont fournis avec loyauté, discrétion et impartialité.
- Le personnel n'utilise que des méthodes, des outils et des techniques validés par le Prestataire de services.
- Le personnel s'engage à ne pas divulguer à un tiers aucune information, même anonymisée et décontextualisée, obtenue ou générée dans le cadre du service VID, sauf autorisation formelle et écrite du Client.
- Le personnel s'engage à informer le Prestataire de services de tout contenu illicite découvert lors du service VID.
- Le personnel s'engage à respecter les lois et règlements en vigueur ainsi que les bonnes pratiques en rapport avec ses activités.

IDnow fait signer à l'ensemble de son personnel le code éthique prévu dans l'exigence décrite ci-dessus avant d'effectuer le service.

IDnow veille au respect du code de déontologie et prévoit des mesures disciplinaires à l'encontre des opérateurs, des administrateurs et des spécialistes de la fraude du service de vérification qui ont enfreint les règles de sécurité ou le code de déontologie.

3.4. PROCÉDURES D'ENREGISTREMENT DES AUDITS

Des fichiers d'audit sont générés par IDnow pour tous les événements liés à la sécurité et aux services VID. Dans la mesure du possible, les journaux d'audit de sécurité sont collectés automatiquement. Lorsque cela n'est pas possible, un registre, un formulaire papier ou un autre mécanisme physique est utilisé. Tous les journaux d'audit de sécurité, qu'ils soient électroniques ou non, sont conservés et mis à disposition lors des audits de conformité. Les journaux contiennent également les informations suivantes :

- le démarrage et l'arrêt des fonctions d'enregistrement ; et
- la disponibilité et l'utilisation des services nécessaires avec le réseau de l'AR ; et
- le démarrage et l'arrêt du système ; et
- les pannes de système et les défaillances matérielles ; et
- activités du pare-feu et du routeur

IDnow utilise un système de journalisation et de surveillance externe qui est protégé contre les accès non autorisés. La journalisation est contrôlée régulièrement pour les données critiques ou

personnelles. Les journaux et la surveillance sont régulièrement vérifiés pour détecter toute anomalie. Un administrateur système vérifie les journaux en cas d'incident de sécurité.

IDnow procède elle-même à des audits de sécurité interne de tous les systèmes et réseaux afin de détecter les vulnérabilités. Ces audits sont réalisés au moins deux fois par an. Le responsable de la sécurité informatique en est chargé.

Toute modification, suppression ou copie de données est enregistrée à l'aide de fichiers journaux par le biais du logiciel IDnow, de sorte que les modifications des données personnelles sont toujours traçables. L'affectation aux comptes appropriés des employés et des clients est garantie à tout moment.

En outre, il est garanti que IDnow enregistre les événements suivants :

- Accès physique aux installations
- Modifications des rôles de confiance
- Gestion des sauvegardes
- Gestion des journaux
- Date, heure, numéro de téléphone utilisé, interlocuteurs et résultats finaux des processus de vérification
- Acceptation et rejet des demandes de certificat
- la gestion des technologies de l'information et des réseaux, en ce qui concerne les systèmes RA
- Gestion de la sécurité

En outre, IDnow enregistre toutes les informations suivantes :

- La preuve de la VID et le RVID qui sont décrits dans la section 2 ci-dessus.
- Tous les traitements et actions automatisés réalisés par les opérateurs et les spécialistes de la fraude dans le cadre d'un contrôle d'identité à distance ; ils sont centralisés sur un composant du système d'information du service auquel les opérateurs et les spécialistes de la fraude n'ont pas accès.
- Toutes les actions menées par les Opérateurs et les spécialistes de la fraude sont disponibles à des fins d'audit.
- La liste de tous les Opérateurs et Administrateurs autorisés à inscrire et à gérer des Utilisateurs.

IDnow met en corrélation les journaux entre les différents composants du système d'information sur les services de VID.

IDnow procède à un examen par échantillonnage des journaux, y compris les opérations effectuées par les Opérateurs et les référents de la fraude.

3.5. ARCHIVAGE DU DOSSIER

Le stockage à long terme garantit que,

- Tous les supports utilisés pour l'archivage sont protégés contre les dommages et les accès non autorisés.
- Les médias sont disponibles pour la durée de vie requise
- Tous les supports sont correctement éliminés à la fin de leur durée de vie.

Les détails du processus de VID, tels que les résultats des contrôles effectués, les employés impliqués et les applications utilisées, sont archivés par IDnow dans un dossier de preuve. Ces procédures s'appliquent à toutes les données personnelles.

La durée de conservation du dossier de preuve de la VID tient compte de la durée pendant laquelle un litige peut survenir. La durée de conservation est définie dans chaque contrat pour chaque Client en fonction de ses besoins. Le processus de destruction des données est défini dans la politique appropriée. Seul l'accès aux données dans le dossier de preuve exigé par le RGPD est fourni conformément à la loi. Si les données doivent être rectifiées, l'identification doit être répétée.

Les résultats de l'identification ("succès" ou "échec"), l'heure de l'identification sont conservés sans limite de temps.

Dès que le dossier de preuve est généré, IDnow le chiffre.

3.6. REPRISE APRÈS SINISTRE

IDnow procède régulièrement à une analyse des risques afin d'identifier tout risque et toute contre-mesure dans les activités et les processus qui couvrent les actifs pertinents pour les services de VID. En tenant compte des résultats de l'évaluation des risques, IDnow sélectionne les mesures techniques ou organisationnelles appropriées de traitement des risques à mettre en œuvre. Les risques sont régulièrement examinés et révisés. Le conseil d'administration est chargé d'approuver l'évaluation des risques et l'acceptation des risques résiduels. En outre, IDnow a défini un processus de gestion des incidents.

IDnow s'assure que toutes les données nécessaires aux opérations de VID, les informations essentielles et les logiciels sont sauvegardés et stockés en lieu sûr, à plus de 5 km du site principal, de manière à permettre à IDnow de reprendre les opérations en temps voulu en cas d'incident/désastre.

Les dispositifs de sauvegarde sont régulièrement testés pour s'assurer qu'ils répondent aux exigences des plans de continuité des activités et qu'ils sont exécutés par les personnes de confiance concernées.

IDnow dispose d'un plan de continuité des activités (PCA) qui énumère les risques applicables, les mesures correctives et les délais de rétablissement acceptables. Un élément clé du PCA est également la manière d'éviter la répétition de la cause qui a déclenché le PCA.

IDnow élabore et met en œuvre un plan de sauvegarde et de récupération pour les dispositifs de service VID, comprenant au minimum la sauvegarde du système, de la configuration et des données.

IDnow définit et met en œuvre des mesures pour garantir la confidentialité et l'intégrité des sauvegardes au même niveau que celui pour lequel le service VID a été approuvé.

IDnow teste le plan de sauvegarde et de récupération au moins une fois par an.

Des informations détaillées sont disponibles dans la "Politique de sécurité d'IDnow", chapitre 9.2, "Gestion des incidents d'IDnow" et "Évaluation des risques d'IDnow Signature électronique qualifiée VideoIdent", chapitre 7.3 "Risques résiduels".

3.6.1. PROCÉDURES DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSION

Les incidents sont soumis via les contacts définis dans la présente Politique de vérification d'identité à distance et traités dans le cadre de la gestion des services. Pour toute vulnérabilité, compte tenu de l'impact potentiel, IDnow crée et met en œuvre un plan d'atténuation de la vulnérabilité ou documente la base factuelle de la détermination que la vulnérabilité ne nécessite pas de remédiation. Les vulnérabilités critiques sont traitées dans les 48 heures suivant leur découverte.

IDnow informera sans délai excessif, mais en tout état de cause dans les 24 heures après en avoir pris connaissance, l'organe de surveillance et, le cas échéant, d'autres organismes compétents de toute violation de la sécurité ou perte d'intégrité ayant un impact significatif sur le service fiduciaire fourni. Le responsable de la sécurité informatique est chargé de cette procédure dans le cadre de sa responsabilité générale en matière de sécurité.

IDnow informera également les personnes physiques lorsqu'une violation de la sécurité ou une perte d'intégrité est susceptible de leur porter préjudice dans un délai raisonnable.

L'ANSSI est alertée par le responsable de la sécurité d'IDnow dans les 24 heures suivant la connaissance de l'incident majeur affectant la sécurité du service VID ou des données personnelles conformément à la procédure de l'ANSSI.

3.7. RÉSILIATION

Au moment où IDnow notifie l'interruption de ses services VID, IDnow s'engage à

- Informer rapidement l'ANSSI et les Clients et mettre en œuvre les activités de démantèlement sur la base du contrat conclu avec le Client.
- Restituer ou détruire toutes les clés, clés API, etc. existantes et reçues à titre privé jusqu'à la fin des opérations, à l'exception des clés utilisées pour chiffrer le dossier de preuve.
- Autoriser les Clients allemands à conserver le dossier de preuve et à suivre les instructions données par l'ANSSI concernant les dossiers de preuve.
- Protéger les dossiers de preuve avec le même niveau de sécurité que celui décrit dans la présente politique de vérification d'identité à distance en attendant leur transfert selon le plan convenu avec l'ANSSI.
- Arrêter d'envoyer des RVID au service commercial, et
- Informer les partenaires commerciaux, dans la mesure où ils sont concernés par la fermeture du domaine d'activité.

IDnow vise à réduire les perturbations potentielles résultant de la cessation des services VID. IDnow dispose d'un plan interne de cessation d'activité à jour.

IDnow a pris des dispositions pour couvrir les coûts liés au respect de ces exigences minimales au cas où IDnow ferait faillite ou, pour d'autres raisons, ne serait pas en mesure de couvrir les coûts par ses propres moyens.

4. CONTRÔLES DE SÉCURITÉ TECHNIQUE

4.1. PROTECTION DES CLÉS PRIVÉES ET INGÉNIERIE DES MODULES CRYPTOGRAPHIQUES

La clé utilisée pour crypter les données du dossier de preuve et le résultat PVID est protégé par un HSM certifié FIPS 140-2 niveau 3 ou EAL 4+ CC. Le HSM est configuré par une personne autorisée par IDnow dans un rôle de confiance uniquement. Le HSM utilise un schéma MofN, demandant au moins 2 personnes distinctes dans un rôle de confiance d'IDnow, pour protéger l'accès à la clé utilisée dans le HSM et pour restaurer la sauvegarde de la clé à l'intérieur d'un SHM configuré avec le même secret que l'initial. Seul le processus technique autorisé peut utiliser la clé dans la production.

4.2. CONTRÔLES DE SÉCURITÉ INFORMATIQUE

IDnow applique toutes les règles du niveau standard du guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service VID.

4.2.1. EXIGENCES TECHNIQUES SPÉCIFIQUES EN MATIÈRE DE SÉCURITÉ INFORMATIQUE

La gestion des utilisateurs est effectuée pour tous les systèmes de traitement des données qui nécessitent une protection. La gestion des utilisateurs s'effectue uniquement à l'aide de comptes personnels. Aucun compte de collecte impersonnel n'est utilisé.

Les lignes directrices générales relatives à la création de mots de passe (telles que la longueur minimale et la complexité du mot de passe) constituent la base de la politique en matière de mots de passe. Tous les employés sont informés de la bonne utilisation des mots de passe et ont signé une directive appropriée.

Il existe un délai d'attente défini pour les sessions.

La conscience de la sécurité de leur environnement de travail est rafraîchie pour tous les employés lors de formations régulières de sensibilisation à la sécurité.

Seuls les administrateurs du système peuvent accéder au système du serveur et toujours par le biais de connexions cryptées. Tous les accès sont personnalisés et protégés par des mots de passe et une authentification à double facteurs.

Les exigences de sécurité doivent être analysées au cours de la phase de conception et de spécification des exigences des projets de développement de systèmes, afin de garantir que la sécurité est intégrée dans les systèmes informatiques.

Les composants du réseau sont placés dans des racks verrouillés afin de les sécuriser physiquement. Les réseaux utilisés pour les services d'identification sont logiquement séparés des autres composants afin d'empêcher tout accès non autorisé. Des pares-feux protègent ces réseaux contre les attaques et les accès non autorisés. La configuration et les mesures de renforcement de ces composants sont régulièrement révisées.

Les comptes administratifs sont utilisés à des fins administratives uniquement.

La direction des ressources humaines délivre aux supérieurs respectifs les droits appropriés qui sont spécifiés conformément aux processus des ressources humaines. Les droits sont ensuite examinés par le responsable de la sécurité informatique. En cas de départ de l'entreprise, les droits d'accès sont retirés dans un délai maximum de 24 heures.

Les détails se trouvent dans la "Politique de sécurité d'IDnow", chapitre 7.

4.2.2 CONTRÔLES TECHNIQUES DU CYCLE DE VIE

Les exigences de cette section s'appliquent à tous les logiciels qui contribuent au traitement de l'acquisition et de la vérification des données d'identification (visage et document d'identité) dans le RVID, à la création du dossier de preuve et à la soumission du RVID à l'unité opérationnelle.

Le département R&D d'IDnow développe et teste régulièrement de nouvelles contre-mesures contre les attaques. En outre, IDnow a mis en place des processus pour s'assurer que les informations sur les cas de fraude non détectés sont reçues de la part des Clients, des Utilisateurs ou des autorités chargées de l'application de la loi. Des détails sont disponibles dans la politique de gestion de la qualité d'IDnow.

Le logiciel doit faire l'objet de révisions régulières du code.

Le logiciel doit être testé pour vérifier qu'il n'y a pas de régression avant qu'une nouvelle version ne soit publiée.

Le logiciel doit faire l'objet d'une procédure de mise à disposition documentée pour chaque version à mettre à disposition.

Le logiciel doit générer des journaux d'enregistrement appropriés pour corréler les enregistrements entre les différents processus du département.

Le développeur du logiciel doit être conscient des risques spécifiques liés au domaine de la vérification d'identité et être tenu à une obligation de discrétion.

Le développement du logiciel doit être effectué dans des conditions qui permettent d'enregistrer les actions de chaque développeur et de les consulter à des fins d'audit.

Chaque fournisseur de logiciel est tenu d'informer le Prestataire de services de toute fraude ou attaque interne visant à altérer le logiciel fourni.

4.2.3 ACCÈS À LA PRODUCTION

L'Administrateur et l'Opérateur n'utilisent que 2 FA et un VPN pour accéder à distance au service VID. Les Administrateurs et Opérateurs sont authentifiés avec un minimum de deux facteurs sur leurs postes de travail nomades. IDnow restreint l'accès des Opérateurs au système d'information du service VID à ce qui est strictement nécessaire à l'exécution de leurs tâches.

Les postes de travail des administrateurs, des opérateurs et des référents fraude sont connectés exclusivement au système d'information du service VID.

Si l'accès à l'internet ou à d'autres systèmes d'information (par exemple, le système d'information interne du fournisseur) est nécessaire, les administrateurs et les opérateurs disposent d'un poste de travail séparé déployé dans une zone extérieure au système d'information du service VID.

IDnow met en place une passerelle dédiée pour l'accès à distance de l'Administrateur et de l'Opérateur conformément à [NT_ADMIN].

Les stations mobiles utilisées par les Administrateurs et les Opérateurs sont dédiées aux services VID.

Les postes de travail mobiles disposent d'une solution de filtrage qui n'autorise que les flux strictement nécessaires, conformément à la politique de filtrage du service de vérification d'identité à distance.

Les postes de travail mobiles ne permettent que l'utilisation de supports amovibles autorisés par la politique de sécurité d'IDnow.

Les postes de travail mobiles ont tous leurs disques cryptés avec des mécanismes cryptographiques conformes à [CRYPTO_B1].

Pour chaque recommandation du guide [NOMADISM], IDnow indique dans la DPVID s'il se conforme ou non à la recommandation. Pour chaque recommandation qu'IDnow déclare respecter, l'entreprise décrit les mesures mises en place pour se conformer à la recommandation. Pour chaque recommandation que l'IDnow déclare ne pas respecter, l'IDnow fournit une justification dans la DPVID.

Les postes de travail mobiles sont configurés de manière à ne pouvoir communiquer avec la passerelle d'accès à distance que par le biais d'une connexion IPsec chiffrée et authentifiée (tunneling complet).

Toutes les informations secrètes échangées dans les protocoles d'authentification sont protégées par cryptographie pendant le transit. Deux ou plusieurs références mettant en œuvre différents facteurs d'authentification sont utilisées (par exemple, quelque chose que vous avez combiné à quelque chose que vous connaissez).

4.3. CONTRÔLES DE SÉCURITÉ DU RÉSEAU

La connexion au service commercial est effectuée via TLS et le service commercial et le service VID sont mutuellement authentifiés.

IDnow développe et maintient une description détaillée de l'architecture du système d'information du service VID. Le système d'information est exclusivement dédié au service de vérification d'identité à distance et tous les autres services sont exécutés sur un système d'information qui est physiquement séparé du système d'information du service.

IDnow élabore et tient à jour la matrice des flux du service VID et la politique de filtrage associée, qui n'autorisent que les flux strictement nécessaires au fonctionnement du service VID. IDnow identifie dans la description détaillée de l'architecture du système d'information du service de VID toutes les interconnexions du système d'information du service de VID avec les systèmes d'information de tiers, y compris le système d'information du service commercial. IDnow filtre tous les flux aux interconnexions du système d'information du service de vérification d'identité à distance.

Tous les systèmes utilisent des scanners de virus qui fonctionnent automatiquement en arrière-plan et sont également mis à jour automatiquement.

IDnow utilise des passerelles de sécurité (pare-feu) ou, si nécessaire, des solutions supplémentaires appropriées telles que des pares-feux d'application, des pare-feu de nouvelle génération, etc. qui, à

leur tour, peuvent effectuer (par exemple par des balayages de ports, etc.) la prévention ou la détection des intrusions.

Des contrôles de sécurité sont effectués, par exemple au moyen d'analyses de vulnérabilité suivies d'une évaluation :

- au moins une fois par trimestre ou
- si IDnow reçoit une demande d'analyse de vulnérabilité de la part de l'AC ou du forum AC/navigateur ou
- après toute modification du système ou du réseau que l'AC juge importante.

Les analyses de vulnérabilité seront effectuées par une société externe spécialisée.

En outre, IDnow effectue des tests de pénétration par l'intermédiaire d'une société spécialisée externe :

- au moins une fois par an ou
- si IDnow reçoit une demande de test de pénétration de la part de l'AC ou du forum AC/navigateur ou
- après toute modification du système ou du réseau que l'AC juge importante.

Toutes les données personnelles envoyées entre le centre d'identification et le centre de données sont cryptées par le biais d'un VPN et, en outre, de TLS. Le réseau de traitement des données d'identification est physiquement séparé du réseau des bureaux.

Le transfert des données vers le client est toujours crypté (TLS, SFTP, S/MIME, etc.).

Le transfert de données entre l'Utilisateur et IDnow lors de l'identification est également toujours crypté (TLS, DTLS pour la vidéo).

Il n'y a pas de transport physique de données.

IDnow garantit le fonctionnement sécurisé de tous les systèmes techniques en les renforçant. Cela comprend en particulier

- Suppression des logiciels/services inutiles
- Suppression des comptes inutiles
- Modifier la configuration en matière de sécurité
- Si nécessaire, activation des composants de sécurité
- Protection des ports du réseau

Les détails peuvent être consultés dans la "Politique de sécurité d'IDnow", chapitre 7.

4.4 HORODATAGE

Tous les systèmes ont leur heure avec une référence de fuseau horaire par rapport à l'UTC synchronisée par NTP au moins une fois par jour.

5. AUDIT DE CONFORMITÉ ET AUTRES ÉVALUATIONS

Avant de jouer le rôle de Prestataire de vérification d'identité à distance, un auditeur externe doit confirmer la conformité au Référentiel PVID de l'ANSSI.

Le service VID ne peut être utilisé qu'après un premier audit réussi réalisé par un auditeur externe accrédité par l'ANSSI. La certification est valable au maximum 2 ans, et avant la date d'expiration de la certification IDnow est audité par un auditeur externe accrédité par l'ANSSI.

En outre, IDnow dispose d'un plan d'audit interne pour contrôler l'ensemble du service VID afin de s'assurer que la politique de sécurité d'IDnow, la politique de vérification d'identité à distance et la DPVID sont appliqués.

IDnow révise le plan de contrôle au moins une fois par an et en cas de modifications structurelles du système d'information du service de VID, y compris des modifications de son hébergement, de son infrastructure et de son architecture, ou en cas de modifications structurelles de l'évaluation des risques d'IDnow, du plan de traitement des risques, de la politique de sécurité d'IDnow, de la politique de vérification d'identité à distance ou de la déclaration de DPVID.

IDnow met à jour le plan de traitement des risques afin d'y intégrer les résultats des contrôles. IDnow fait valider formellement et par écrit les résultats des contrôles par sa direction.

En cas de constatations majeures faites au cours de l'audit interne par l'auditeur accrédité ou par le Client, il convient d'y remédier et un audit externe sera réalisé au cours de la même année afin de vérifier les constatations.

La politique de vérification d'identité à distance pour cet OID est couverte par un audit de l'ANSSI conformément au référentiel PVID de l'ANSSI.

6. AUTRES AFFAIRES ET QUESTIONS JURIDIQUES

6.1. RESPONSABILITÉ FINANCIÈRE

IDnow dispose de ressources financières suffisantes et a souscrit une assurance responsabilité civile appropriée, conformément à la législation applicable, pour couvrir les responsabilités découlant de ses opérations et/ou activités.

6.2. CONFIDENTIALITÉ DES INFORMATIONS PERSONNELLES

IDnow dispose d'un plan de confidentialité qui est présenté à l'Utilisateur au début du processus et qui doit être confirmé par l'Utilisateur. Le plan de confidentialité est conforme au RGPD.

L'Utilisateur ne peut exercer son droit d'accès à ses données à caractère personnel telles qu'énumérées à l'article 2.6. L'Utilisateur ne peut avoir accès à aucun autre type de données ayant fait l'objet d'un traitement automatisé ou manuel ou dont la communication est susceptible de fournir des informations sur la nature des contrôles effectués par le service et relatifs à la détection de l'usurpation d'identité.

L'Utilisateur ne peut pas demander la modification ou la suppression des données à caractère personnel contenues dans le dossier de preuve car il s'agit d'une preuve qui doit être conservée par IDnow en tant que PVID RIV et le cas échéant, une preuve pouvant être demandée par le Client pour vérifier l'identité de l'Utilisateur par IDnow en tant que PVID.

Le Client doit communiquer à l'Utilisateur la durée de conservation des données à caractère personnel de l'Utilisateur. Les données à caractère personnel contenues dans le dossier de preuve ne peuvent être supprimées qu'à l'issue de la période de conservation définie par le Client. Quel que soit le verdict (succès ou échec), le dossier de preuve (qui contient toutes les données personnelles énumérées dans la section 2, y compris le RVID) est enregistré par IDnow selon une période de conservation définie par le Client.

Toutes les données d'identification énumérées dans la section 2 ci-dessus sont collectées et stockées à des fins de preuve, de vérification de l'identité de l'Utilisateur et de transmission du RVID à un Client et, dans certains cas, de transmission du dossier de preuves à certains Clients allemands spécifiques, en respectant le principe de minimisation des données collectées et conservées conformément au RGPD.

Toutes les données énumérées à la section 2 ci-dessus ne sont pas utilisées dans le cadre d'un traitement biométrique.

IDnow peut, travailler conformément à un accord de traitement des données commandé avec le Client. Le Client est alors l'entité responsable de traitement au sens de l'Art. 4 n° 7 du RGPD. Le sous-traitant doit respecter les principes d'un traitement correct des données. Le sous-traitant doit garantir les mesures de sécurité de l'information convenues par contrat et prescrites par la loi, en particulier le respect des principes énoncés à l'article 5 I lit. f, 25 et 26 du RGPD. 5 I lit. f, 25 et 32 RGPD.

IDnow héberge et traite les données personnelles relatives au service VID exclusivement sur le territoire d'un État membre de l'Union européenne. L'Opérateur et l'Administrateur, ainsi que le centre de données utilisé pour héberger et gérer le service VID, sont exclusivement situés sur le territoire d'un État membre de l'Union européenne.

En outre, IDnow a nommé Délégué protection des données.

Chaque nouvel agent, nouvellement recruté chez IDnow, suit une formation sur la protection de la vie privée pendant sa période d'activité et passe un test en ligne sur la protection des données.

6.3. DÉCLARATIONS ET GARANTIES

IDnow s'assure, en tant que PPVID, que chaque Utilisateur a été identifié et authentifié correctement avant de transmettre le RVID, quel que soit le verdict. En outre, IDnow est responsable de l'exécution et de l'autorisation correctes du service VID. À cet effet, IDnow utilise un large éventail de contrôles automatisés qui sont effectués par le logiciel IDnow ainsi que d'autres contrôles manuels effectués par un Opérateur formé.

Avant de s'inscrire à un service VID, l'Utilisateur peut consulter les conditions générales d'utilisation du service VID. En outre, l'Utilisateur doit accepter ces conditions générales en cliquant sur une case à cocher affichée à l'écran. L'Utilisateur peut accéder aux conditions générales via le site web d'IDnow.

IDnow veille à ce que les données contenues dans le RVID soient complètes et exactes. IDnow soutient les équipes d'audit et doit faire tout ce qui est raisonnablement possible pour mener à bien un audit et en communiquer les résultats.

IDnow garantit que les enregistrements concernant le fonctionnement des services seront mis à disposition si cela est nécessaire pour fournir la preuve du bon fonctionnement des services dans le cadre d'une procédure judiciaire.

6.4. LIMITATIONS DE RESPONSABILITÉ

IDnow garantit avoir effectué le processus de VID et la transmission du RVID au Client selon le niveau de risque pour le service VID associé au niveau substantiel uniquement.

IDnow n'est pas responsable de l'adéquation ou de l'authenticité de l'opération réalisée par le Client en vertu de la présente politique VID sur la base de l'utilisation du RVID.

6.5. INDEMNITÉS

IDnow ne fait aucune déclaration quant à l'adéquation de l'opération réalisée par le Client en vertu de la présente politique VID basée sur l'utilisation du RVID à quelque fin que ce soit. Les parties utilisatrices utilisent le RVID et les opérations basées sur le RVID à leurs propres risques. IDnow n'a aucune obligation d'effectuer des paiements concernant les coûts associés au dysfonctionnement ou à la mauvaise utilisation du RVID émis dans le cadre de la présente politique VID.

6.6. DISPOSITIONS RELATIVES AU RÈGLEMENT DES LITIGES

En cas de litige, les parties trouveront un accord en tenant compte des lois, règlements et accords applicables.

IDnow met à la disposition du Client, de l'Utilisateur et des tiers un processus d'enregistrement et de traitement des plaintes concernant le service VID. Pour tous les litiges liés à l'identification de l'Utilisateur, l'autorité d'enregistrement IDnow GmbH peut être contactée directement à l'adresse support@mail.idnow.de. Pour tous les litiges liés à l'Utilisateur ou à un tiers, l'équipe chargée de la réussite des Clients peut être contactée à l'adresse électronique fournie lors de l'intégration du Client.

6.7. DROIT APPLICABLE

Le droit français s'applique.

6.8. DISPOSITIONS DIVERSES

IDnow exerce ses activités conformément à la loi allemande sur la non-discrimination.

ANNEXE 1 : DOCUMENTS D'IDENTIFICATION AUTORISÉS

Seuls les documents d'identité suivants sont acceptés dans le cadre de la présente norme, à condition qu'ils présentent les caractéristiques nécessaires pour satisfaire aux exigences énoncées dans la présente norme :

a) Pour les ressortissants des États membres de l'Union européenne, d'un État partie à l'accord sur l'Espace économique européen ou de la Suisse, le passeport ou la carte d'identité.

(b) Pour les ressortissants de pays tiers résidant dans un État membre de l'Union européenne, dans un État partie à l'accord sur l'Espace économique européen ou en Suisse, le titre de séjour, établi conformément au modèle prévu par le règlement (UE) n° 2017/1954 du Parlement européen et du Conseil du 25 octobre 2017 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, délivré par l'État de résidence.

(c) Pour les ressortissants de pays tiers exemptés de l'obligation de visa de court séjour qui ne résident pas sur le territoire de l'Union européenne, dans un État partie à l'accord sur l'Espace économique européen ou en Suisse, le passeport, à condition que le pays de délivrance mette à disposition les moyens nécessaires pour vérifier la validité du document. Si l'exemption de l'obligation de visa est assortie de l'obligation de disposer d'un passeport électronique, seul le passeport électronique est reconnu comme source faisant foi pour le pays concerné.

(d) Pour les ressortissants de pays tiers qui sont réfugiés ou reconnus comme apatrides ou comme bénéficiaires de la protection prévue par la directive 2011/95/UE du Parlement européen et du Conseil du 13 décembre 2011 concernant les normes relatives aux conditions que doivent remplir les ressortissants des pays tiers ou les apatrides pour pouvoir bénéficier d'une protection internationale, et relatives au contenu de cette protection, le passeport est remplacé par le document de voyage délivré par l'État qui a reconnu le statut de réfugié ou d'apatride ou qui a accordé la protection.

ANNEXE 2 : LISTE DES DOCUMENTS D'IDENTIFICATION AUTORISÉS

Code pays	Nom du pays	Nom du document	PRADO Référence
AD	Andorre	Passeport 2017	AND-AO-03001
AE	Émirats arabes unis	Passeport 2011	UAE-AO-02001
AF	Afghanistan	Passeport 2016	AFG-AO-01002
AF	Afghanistan	Passeport 2017	AFG-AO-04001
AM	Arménie	Passeport 2012	ARM-AO-02001
AO	Angola	Passeport 2000	AGO-AO-01001
AR	Argentine	Passeport 2012	ARG-AO-03001
AT	Autriche	Passeport 2006	AUT-AO-02001
AT	Autriche	Passeport 2014	AUT-AO-02002
AT	Autriche	Carte d'identité 2010	AUT-BO-02003
AT	Autriche	Carte d'identité 2021	AUT-BO-03001
AT	Autriche	Permis de séjour 2012	AUT-HO-05001
AT	Autriche	Permis de séjour 2012	AUT-HO-05002
AT	Autriche	Permis de séjour 2012	AUT-HO-05003
AT	Autriche	Permis de séjour 2015	AUT-HO-06001
AT	Autriche	Permis de séjour 2015	AUT-HO-06002
AT	Autriche	Permis de séjour 2015	AUT-HO-06003
AT	Autriche	Permis de séjour 2013	AUT-HO-07001
AT	Autriche	Permis de séjour 2013	AUT-HO-07002
AT	Autriche	Permis de séjour 2013	AUT-HO-07003
AT	Autriche	Permis de séjour 2014	AUT-HO-14001
AT	Autriche	Permis de séjour 2014	AUT-HO-14002
AU	Australie	Passeport 2009	AUS-AO-04001
AU	Australie	Passeport 2014	AUS-AO-05001
AZ	Azerbaïdjan	Passeport 2013	AZE-AO-02002
BA	Bosnie et Herzégovine	Passeport 2010	BIH-AO-02001
BA	Bosnie et Herzégovine	Passeport 2014	BIH-AO-03001
BA	Bosnie et Herzégovine	Carte d'identité 2013	BIH-BO-03001
BD	Bangladesh	Passeport 2013	BGD-AO-03001
BE	Belgique	Passeport 2008	BEL-AO-07003
BE	Belgique	Passeport 2014	BEL-AO-08001
BE	Belgique	Passeport 2017	BEL-AO-09003
BE	Belgique	Passeport 2019	BEL-AO-10003
BE	Belgique	Passeport 2022	BEL-AO-11001
BE	Belgique	Passeport 2023	BEL-AO-11002
BE	Belgique	Carte d'identité 2010	BEL-BO-07001
BE	Belgique	Carte d'identité 2010	BEL-BO-08001

BE	Belgique	Carte d'identité 2015	BEL-BO-09001
BE	Belgique	Carte d'identité 2015	BEL-BO-09002
BE	Belgique	Carte d'identité 2015	BEL-BO-09003
BE	Belgique	Carte d'identité 2020	BEL-BO-10001
BE	Belgique	Carte d'identité 2021	BEL-BO-10002
BE	Belgique	Carte d'identité 2021	BEL-BO-11001
BE	Belgique	Carte d'identité 2021	BEL-BO-11004
BE	Belgique	Permis de séjour 2013	BEL-HO-08001
BE	Belgique	Permis de séjour F - flamand	BEL-HO-09001
BE	Belgique	Permis de séjour F - français	BEL-HO-09002
BE	Belgique	Permis de séjour F - allemand	BEL-HO-09003
BE	Belgique	Permis de séjour F plus - flamand	BEL-HO-10001
BE	Belgique	Permis de séjour F plus - français	BEL-HO-10002
BE	Belgique	Permis de séjour F plus - allemand	BEL-HO-10003
BE	Belgique	Permis de séjour E - flamand	BEL-HO-11001
BE	Belgique	Permis de séjour E - français	BEL-HO-11002
BE	Belgique	Permis de séjour E - allemand	BEL-HO-11003
BE	Belgique	Permis de séjour E plus - flamand	BEL-HO-12001
BE	Belgique	Permis de séjour E plus - français	BEL-HO-12002
BE	Belgique	Permis de séjour E plus - allemand	BEL-HO-12003
BF	Burkina Faso	Passeport 2013	BFA-AO-03001
BG	Bulgarie	Passeport 2010	BGR-AO-02001
BG	Bulgarie	Carte d'identité 2010	BGR-BO-02001
BI	Burundi	Passeport 2018	BDI-AO-02001
BR	Brésil	Passeport 2010	BRA-AO-02001
CA	Canada	Passeport 2013	CAN-AO-04001
CH	Suisse	Passeport 2010	CHE-AO-03002
CH	Suisse	Passeport 2022	CHE-AO-04001
CH	Suisse	Carte d'identité 2005	CHE-BO-01003
CH	Suisse	Carte d'identité 2023	CHE-BO-02001
CI	Côte d'Ivoire	Passeport 2008	CIV-AO-02001
CN	Chine	Hong Kong 2007	CHN-AO-03003
CN	Chine	Hong Kong 2019	CHN-AO-03004
CN	Chine	Macao 2009	CHN-AO-04003
CN	Chine	Passeport 2012	CHN-AO-05001
LE CO	Colombie	Passeport 2010	COL-AO-02001
LE CO	Colombie	Passeport 2019	COL-AO-04001
CY	Chypre	Passeport 2009	CYP-AO-04001
CY	Chypre	Carte d'identité 2015	CYP-BO-04001

CY	Chypre	Carte d'identité 2020	CYP-BO-04002
CY	Chypre	Permis de séjour 2020	CYP-HO-05001
CZ	République tchèque	Passeport 2006	CZE-AO-04001
CZ	République tchèque	Carte d'identité 2012	CZE-BO-04001
CZ	République tchèque	Carte d'identité 2014	CZE-BO-04002
CZ	République tchèque	Carte d'identité 2021	CZE-BO-04003
DE	Allemagne	Passeport 2007	DEU-AO-01006
DE	Allemagne	Passeport 2007	DEU-AO-01007
DE	Allemagne	Passeport 2017	DEU-AO-04001
DE	Allemagne	Carte d'identité 2010	DEU-BO-02001
DE	Allemagne	Carte d'identité 2021	DEU-BO-02004
DE	Allemagne	Permis de séjour 2011	DEU-HO-21001
DE	Allemagne	Permis de séjour 2011	DEU-HO-21002
DE	Allemagne	Permis de séjour 2011	DEU-HO-21003
DE	Allemagne	Permis de séjour 2019	DEU-HO-22003
DE	Allemagne	Permis de séjour 2021	DEU-HO-22005
DJ	Djibouti	Passeport DJI 2017	DJI-AO-02001
DK	Danemark	Passeport 2004	DKN-AO-04001
DK	Danemark	Passeport 2004	DKN-AO-05001
DK	Danemark	Passeport 2004	DKN-AO-05002
DK	Danemark	Passeport 2004	DKN-AO-05003
DK	Danemark	Passeport 2004	DNK-AO-03001
DK	Danemark	Passeport 2020	DNK-AO-06001
DZ	Algérie	Passeport 2012	DZA-AO-01001
EE	Estonie	Passeport 2007	EST-AO-02005
EE	Estonie	Passeport 2014	EST-AO-03005
EE	Estonie	Passeport 2021	EST-AO-06001
EE	Estonie	Carte d'identité 2011	EST-BO-03001
EE	Estonie	Carte d'identité 2018	EST-BO-04001
EE	Estonie	Carte d'identité 2021	EST-BO-04002
EG	Égypte	Passeport 2008	EGY-AO-01001
ES	Espagne	Passeport 2006	ESP-AO-04001
ES	Espagne	Passeport 2015	ESP-AO-05001
ES	Espagne	Carte d'identité 2006	ESP-BO-03001
ES	Espagne	Carte d'identité 2015	ESP-BO-05001
ES	Espagne	Carte d'identité 2021	ESP-BO-06001
ES	Espagne	Permis de séjour 2011	ESP-HO-02005
ES	Espagne	Permis de séjour 2020	ESP-HO-03001
FI	Finlande	Passeport 2012	FIN-AO-05001
FI	Finlande	Passeport 2012	FIN-AO-05002
FI	Finlande	Passeport 2017	FIN-AO-06001
FI	Finlande	Passeport 2023	FIN-AO-07001
FI	Finlande	Passeport 2023	FIN-AO-07002
FI	Finlande	Carte d'identité 2011	FIN-BO-06001
FI	Finlande	Carte d'identité 2017	FIN-BO-09001

FI	Finlande	Carte d'identité 2021	FIN-BO-11001
FI	Finlande	Carte d'identité 2023	FIN-BO-12001
FI	Finlande	Carte d'identité 2023	FIN-BO-12004
FI	Finlande	Carte d'identité pour mineurs 2017	FIN-BO-10001
FR	France	Passeport 2013	FRA-AO-03003
FR	France	Passeport 2019	FRA-AO-03004
FR	France	Carte d'identité 1994	FRA-BO-02002
FR	France	Carte d'identité 2021	FRA-BO-03001
FR	France	Permis de séjour 2011	FRA-HO-09001
FR	France	Permis de séjour 2020	FRA-HO-12001
GB	Royaume-Uni	Passeport 2010	GBR-AO-04001
GB	Royaume-Uni	Passeport 2015	GBR-AO-05001
GB	Royaume-Uni	Passeport 2020	GBR-AO-06001
GE	Géorgie	Carte d'identité 2011	GEO-BO-01001
GH	Ghana	Passeport 2010	GHA-AO-02001
GN	Guinée	Passeport 2018	GIN-AO-03001
GR	Grèce	Passeport 2006	GRC-AO-03001
GR	Grèce	Passeport 2006	GRC-AO-03002
GR	Grèce	Passeport 2006	GRC-AO-03003
RH	Croatie	Passeport 2009	HRV-AO-02001
RH	Croatie	Carte d'identité 2003	HRV-BO-02001
RH	Croatie	Carte d'identité 2013	HRV-BO-03001
RH	Croatie	Carte d'identité 2015	HRV-BO-03002
RH	Croatie	Carte d'identité 2021	HRV-BO-04001
HU	Hongrie	Carte d'identité 2012 - B	HUN-BO-04001
HU	Hongrie	Carte d'identité 2012 - A	HUN-BO-04002
HU	Hongrie	Carte d'identité 2016	HUN-BO-05001
HU	Hongrie	Carte d'identité 2016	HUN-BO-05002
HU	Hongrie	Carte d'identité 2016	HUN-BO-05003
HU	Hongrie	Carte d'identité 2016	HUN-BO-05004
IE	Irlande	Passeport 2013 - B	IRL-AO-04002
IE	Irlande	Passeport 2013 - A	IRL-AO-05001
IE	Irlande	Carte d'identité 2015	IRL-TO-01002
IL	Israël	Passeport 2012	ISR-AO-03001
IR	République islamique d'Iran	Passeport 2014	IRN-AO-04001
IS	Islande	Passeport 2006	ISL-AO-03001
IS	Islande	Passeport 2019	ISL-AO-05001
IT	Italie	Passeport 2010	ITA-AO-02004
IT	Italie	Carte d'identité 2016	ITA-BO-04004
IT	Italie	Carte d'identité 2022	ITA-BO-04005
JP	Japon	Passeport 2013	JPN-AO-02003
JP	Japon	Passeport 2013	JPN-AO-02004
KE	Kenya	Passeport 2015	KEN-AO-03001

KR	Corée (Sud)	Passeport 2008	KOR-AO-03002
KR	Corée (Sud)	Passeport 2021	KOR-AO-04001
KW	Koweït	Passeport 2016	KWT-AO-01001
KZ	Kazakhstan	Passeport 2010	KAZ-AO-02001
LB	Liban	Passeport 2016	LBN-AO-02001
LI	Liechtenstein	Carte d'identité 2009	LIE-BO-02001
LT	Lituanie	Passeport 2008	LTU-AO-04001
LT	Lituanie	Passeport 2008	LTU-AO-04002
LT	Lituanie	Passeport 2008	LTU-AO-04003
LT	Lituanie	Passeport 2019	LTU-AO-04004
LU	Luxembourg	Passeport 2006	LUX-AO-02003
LU	Luxembourg	Passeport 2015	LUX-AO-02005
LU	Luxembourg	Passeport 2006	LUX-AO-03001
LV	Lettonie	Carte d'identité 2012	LVA-BO-01001
LV	Lettonie	Carte d'identité 2019	LVA-BO-02001
LY	Libye	Passeport 2013	LBY-AO-02001
MA	Maroc	Passeport 2009	MAR-AO-02001
MC	Monaco	Carte d'identité 2009	MCO-BO-01001
MD	Moldavie	Passeport 2014	MDA-AO-01004
MD	Moldavie	Passeport 2018	MDA-AO-05001
MD	Moldavie	Carte d'identité 2015	MDA-BO-02001
MD	Moldavie	Carte d'identité 2015	MDA-BO-02002
ME	Monténégro	Passeport 2008	MNE-AO-02001
MK	Macédoine	Passeport 2007	MKD-AO-03001
ML	Mali	Passeport 2007	MLI-AO-02001
ML	Mali	Passeport 2016	MLI-AO-03002
MR	Mauritanie	Passeport 2013	MRT-AO-01001
MT	Malte	Passeport 2008	MLT-AO-04001
MT	Malte	Carte d'identité 2002	MLT-BO-02001
MT	Malte	Carte d'identité 2014	MLT-BO-03001
MV	Maldives	Passeport 2016	MDV-AO-04001
MW	Malawi	Passeport 2011	MWI-AO-02001
MX	Mexique	Passeport 2016	MEX-AO-03001
MX	Mexique	Passeport 2012	MEX-AO-02004
MON	Malaisie	Passeport 2010	MYS-AO-02001
MON	Malaisie	Passeport 2017	MYS-AO-03001
NG	Nigéria	Passeport 2019	NGA-AO-03001
NL	Pays-Bas	Passeport 2011	NLD-AO-03001
NL	Pays-Bas	Passeport 2014	NLD-AO-04001
NL	Pays-Bas	Passeport 2021	NLD-AO-05001
NL	Pays-Bas	Carte d'identité 2014	NLD-BO-04001
NL	Pays-Bas	Carte d'identité 2017	NLD-BO-05001
NL	Pays-Bas	Carte d'identité 2021	NLD-BO-06001
NL	Pays-Bas	Carte d'identité 2021	NLD-BO-07001
NON	Norvège	Passeport 2011	NOR-AO-04001

NON	Norvège	Passeport 2011	NOR-AO-05001
NON	Norvège	Passeport 2020	NOR-AO-06001
NZ	Nouvelle-Zélande	Passeport 2009	NZL-AO-03002
NZ	Nouvelle-Zélande	Passeport 2021	NZL-AO-04001
PE	Pérou	Passeport 2016	PER-AO-02001
PH	Philippines	Passeport 2010	PHL-AO-02001
PH	Philippines	Passeport 2010	PHL-AO-03001
PH	Philippines	Passeport 2016	PHL-AO-04001
PL	Pologne	Passeport 2006 - B	POL-AO-04001
PL	Pologne	Passeport 2006 - A	POL-AO-05001
PL	Pologne	Passeport 2018	POL-AO-06001
PL	Pologne	Passeport 2022	POL-AO-07001
PL	Pologne	Carte d'identité 2001-2013	POL-BO-02001
PL	Pologne	Carte d'identité 2001-2013	POL-BO-02002
PL	Pologne	Carte d'identité 2001-2013	POL-BO-02003
PL	Pologne	Carte d'identité 2015	POL-BO-03001
PL	Pologne	Carte d'identité 2019	POL-BO-04001
PL	Pologne	Carte d'identité 2021	POL-BO-05001
PL	Pologne	Permis de séjour 2014	POL-HO-11002
PL	Pologne	Permis de séjour 2020	POL-HO-12001
PT	Portugal	Passeport 2009	PRT-AO-01003
PT	Portugal	Passeport 2017	PRT-AO-04001
PT	Portugal	Carte d'identité 2015	PRT-BO-03005
PT	Portugal	Permis de séjour 2008	PRT-HO-02001
PT	Portugal	Permis de séjour 2019	PRT-HO-06001
RO	Roumanie	Passeport 2019	ROU-AO-03001
RO	Roumanie	Carte d'identité 2021	ROU-BO-05001
RS	Serbie	Passeport 2008	SRB-AO-01001
RU	Fédération de Russie	Passeport 2010	RUS-AO-03003
RW	Rwanda	Passeport 2019	RWA-AO-02001
SE	Suède	Passeport 2012	SWE-AO-04001
SE	Suède	Passeport 2022	SWE-AO-05001
SE	Suède	Carte d'identité 2012	SWE-BO-03001
SE	Suède	Carte d'identité 2021	SWE-BO-03002
SE	Suède	Carte d'identité 2022	SWE-BO-04001
SE	Suède	Permis de séjour 2012	SWE-HO-09001
SG	Singapour	Passeport 2006	SGP-AO-04001
SG	Singapour	Passeport 2017	SGP-AO-05001
SI	Slovénie	Passeport 2006	SVN-AO-02001
SI	Slovénie	Passeport 2006	SVN-AO-02002
SI	Slovénie	Passeport 2006	SVN-AO-02003
SI	Slovénie	Passeport 2016	SVN-AO-02004
SI	Slovénie	Carte d'identité 1998	SVN-BO-02001
SK	Slovaquie	Passeport 2008	SVK-AO-03001
SK	Slovaquie	Passeport 2014	SVK-AO-04001

SK	Slovaquie	Carte d'identité 2013	SVK-BO-03001
SK	Slovaquie	Carte d'identité 2013	SVK-BO-04001
SK	Slovaquie	Carte d'identité 2015	SVK-BO-05001
TH	Thaïlande	Passeport 2012	THA-AO-02002
TH	Thaïlande	Passeport 2020	THA-AO-06001
TR	Turquie	Passeport 2010	TUR-AO-02001
TR	Turquie	Passeport 2017	TUR-AO-03001
TW	Taïwan	Passeport 2008	TWN-AO-03001
TW	Taïwan	Passeport 2018	TWN-AO-04001
TW	Taïwan	Passeport 2018	TWN-AO-04002
UA	Ukraine	Passeport 2007	UKR-AO-02001
UA	Ukraine	Passeport 2007	UKR-AO-02002
UA	Ukraine	Passeport 2015	UKR-AO-03001
UA	Ukraine	Passeport 2015	UKR-AO-03002
UA	Ukraine	Carte d'identité 2016	UKR-BO-2016
ÉTATS-UNIS	États-Unis d'Amérique	Passeport 2006	USA-AO-04001
ÉTATS-UNIS	États-Unis d'Amérique	Passeport 2020	USA-AO-05001
VE	Venezuela	Passeport 2011	VEN-AO-02001
XK	Kosovo	Passeport 2013	RKS-AO-03001
XK	Kosovo	Carte d'identité 2013	RKS-BO-02001
ZA	Afrique du Sud	Passeport 2009	ZAF-AO-02001