Politique	
POLITIQUE DU SERVICE DE VÉRIFICATION D'IDENTITÉ À DISTANCE CERTIFIÉ OID : [1.3.6.1.4.1.62466.88.1.2.1.0]	
Objet / Synthèse	POLITIQUE DU SERVICE DE VÉRIFICATION D'IDENTITÉ À DISTANCE CERTIFIÉ CHECKMI

Niveau de diffusion	D3 – Diffusion libre
Liste de diffusion	Public
Localisation	Be Ys Trusted Solutions France

Version	Date	Modifications	Rédacteur
0.1	30/04/2025	Création de base	Ralitsa Ivanova
0.1	13/10/2025	Corrections / Adaptations	Franck Dutertre
0.1	25/03/2026	Ajout de précisions	Franck Dutertre
1.0	13/05/2026	Ajustement du numéro OID suite à typo découvert	Lidiya Ivanova
Date de péremption		2 ans	

Documents de Références

Libellé	**Localisation ou insertion du document**
POL_Politique_PVID_CheckMi_v1.0	**Sharepoint**

Glossaire

Terme / Acronyme	Définition
AC	Autorité de certification
C2SC	Comité de suivi des services de confiance
CGU	Conditions générales d'utilisation
ANSSI	Agence nationale de la sécurité des systèmes d'Information
CNIL	Commission nationale de l'informatique et des libertés
VID	Vérification d'identité à distance
MCO	Maintien en condition opérationnelle
OID	Object Identifier
PVID	Prestataire de vérification d'identité à distance

Définitions

Terme	Définition
Prestataire/PVID	BE YS TRUSTED SOLUTIONS FRANCE
Utilisateur	Personne physique, qui utilise le Service certifié et, notamment dont l'identité a été/est/sera à vérifier
Commanditaire	Entité responsable d'un Service métier ayant recours à un Service de vérification d'identité à distance.
Dossier de preuve	Elément conservé par le Prestataire rassemblant les informations pertinentes à produire pour la résolution des litiges, ou en cas d'enquête et notamment afin de fournir des preuves en justice. Il est expressément convenu que les données contenues dans le Dossier de preuve ne sont pas conservées à des fins de traitement biométrique
Titre d'identité	Document officiel certifiant l'identité d'une personne
Données d'identification	Ensemble de données à caractère personnel (p.ex. la vidéo du visage de l'utilisateur, la vidéo du titre d'identité présenté par l'utilisateur), acquises

	et vérifiées par le Service afin de vérifier l'identité d'une personne physique
Attributs d'identité	Données transmises par le Service de vérification d'identité à distance au Commanditaire. Généralement, ce sont : le nom de naissance, le nom d'usage si présent, le(s) prénom(s), la date de naissance, le lieu de naissance, la nationalité, le genre
Attributs du titre d'identité	Données extraites du titre d'identité présenté permettant d'en contrôler l'authenticité et la validité. Les attributs obligatoires sont le numéro de document, le pays émetteur et la date d'expiration
API (Interface de programme d'application)	Interface logicielle permettant de recourir au Service PVID
Parties prenantes	Personne, machine ou Service participant au processus du Service de confiance
Rôle de confiance	Personnes de confiance, formellement identifiées, qui participent à la réalisation des actions sensibles du Service certifié
Groupe Be Ys	L'entité économique formée par l'ensemble des sociétés contrôlées par BE INVEST International S.A.

Validation

Relecteur	**Fonction (par rapport au document)**
Franck Dutertre	Président C2SC
Stefan Stefanov	Responsable du Service
Approbateur	**Fonction (par rapport au document)**
Bruno Buffenoir	Directeur des services de confiance numérique Bruno Buffenoir Electronically Signed by Bruno Buffenoir 13/05/2026 à 14:00 CEST bevys trusted solutions

Table des matières

1. Introduction

1.1 Présentation générale

BE YS TRUSTED SOLUTIONS FRANCE (BE YS TRUSTED SOLUTIONS) est un prestataire de services de confiance ayant un haut niveau de garantie.

Le Service de vérification d'identité à distance proposé par BE YS TRUSTED SOLUTIONS est certifié par l'ANSSI dans le cadre du référentiel PVID.

Le Service est dédié à la vérification d'identité des personnes physiques et est accessible pour l'Utilisateur au moyen d'une application mise à disposition par le Commanditaire.

Le parcours est divisé en quatre étapes :

- L'acquisition des données d'identification ;
- La vérification des données d'identification ;
- La constitution du dossier de preuve ;
- La transmission du résultat de la vérification d'identité à distance.

La vérification des données d'identification est automatisée, en utilisant des modèles d'IA avancés pour la vérification l'authenticité du document d'identité, la comparaison du visage et la détection du vivant, sans intervention humaine directe. Le verdict final est donné par un Superviseur secondaire humain en se basant sur le résultat du traitement automatique.

Le niveau de garantie « substantiel » assigné au Service, assure un haut degré de fiabilité du résultat de vérification de l'identité à distance et indique sa conformité aux plus hauts standards, procédures et spécifications techniques y correspondant dans le but de prévenir la fuite des données, d'usurpation d'identité, de création de fausse identité et d'altération de données d'identification.

L'organisation adoptée pour cela est présentée dans ce document.

1.2 Politique de vérification d'identité à distance (Politique VID)

Ce document représente la Politique de vérification d'identité à distance (Politique) de BE YS TRUSTED SOLUTIONS. Il identifie les attributs du titre d'identité qui caractérisent l'unicité de l'identité d'une personne physique et décrit l'ensemble de règles définissant les exigences auxquelles le prestataire se conforme, ainsi que les normes qu'il applique dans la mise en place et la fourniture du Service de vérification de données personnelles des personnes physiques et, le cas échéant, de tout attribut spécifique lié à ces personnes.

La Politique identifie également les mesures de sécurité, les obligations et les exigences portant sur les autres intervenants, notamment les Utilisateurs et les Commanditaires et fait partie indissociable des Conditions générales d'utilisation (CGU).

Ce document a été élaboré en conformité avec le Règlement (UE) 2016/679 (RGPD), ainsi que la législation française applicable. La Politique est publique et peut être modifiée par BE YS TRUSTED SOLUTIONS à tout moment.

1.3 Identification et date d'entrée en vigueur de la Politique

1.3.1 Identification du document

Le présent document est identifié par l'OID suivant : [1.3.6.1.4.1.62466.88.1.2.1.0]

1.3.2 Date d'entrée en vigueur

La Politique entre en vigueur après approbation par le Comité de suivi des Services de confiance (C2SC) de BE YS TRUSTED SOLUTIONS et à la date fixée par ce Comité. La Politique est publiée sur le site web : https://www.kipmi.com au moins 72h avant sa date d'entrée en vigueur.

1.3.3 Durée et fin anticipée de validité de la Politique

La Politique du Service reste en application au moins jusqu'à la fin de vie du dernier dossier de preuve constitué.

Le présent document reste en vigueur jusqu'à la publication d'une nouvelle version.

1.4 Gestion de la Politique

1.4.1 Entité gérant la Politique

La présente Politique est gérée par les membres du C2SC du Prestataire.

1.4.2 Point de contact

Le point de contact pour toute question à propos de la Politique est :

- Adresse postale : BE YS TRUSTED SOLUTIONS FRANCE
  Service VID
  10 boulevard Haussmann 75009 Paris France
- Adresse électronique : support@kipmi.com

1.4.3 Procédure d'approbation de la Politique

La Politique est approuvée par le C2SC après examen et relecture du document par les membres du Comité, et par les personnes désignées par celui-ci.

Cette relecture a pour objectif d'assurer :

- La conformité de la Politique avec les exigences réglementaires et normatives portant sur la fourniture du Service certifié ;
- La cohérence de la Politique avec les autres documents publiés dans le cadre du Service, tels par exemple que les Conditions Générales d'Utilisation ;
- La concordance entre les engagements exprimés dans la Politique et les moyens techniques et organisationnels mis en œuvre par le Prestataire et ses partenaires ;

- L'information effective de l'organe de contrôle pour toute modification importante dans la fourniture du Service certifié selon les modalités décrites dans les procédures de certification. Cela comprend notamment, sans s'y limiter :
  - Les changements induits par une modification de la Politique de Service ou des Conditions générales d'utilisation associées ;
  - Les changements de sous-traitants ;
  - Les modifications des conditions d'hébergement ;
  - Les changements de matériels cryptographiques ;
  - Les modifications d'architecture technique ;
  - Les changements de procédures d'enregistrement et d'identification ;
  - Les changements dans la gouvernance du Service.

Le C2SC s'assure que la date d'entrée en vigueur de la nouvelle Politique laisse, dans la mesure du possible, un délai suffisant aux Commanditaires pour prendre connaissance des nouvelles dispositions et adapter si besoin leurs pratiques.

1.5 Informations publiées

1.5.1 Entités chargés de la mise à disposition des informations

Le Prestataire assure la publication d'informations à destination des Commanditaires et des Utilisateurs sur son site web : https://www.kipmi.com/index.php/produits/confiance-numerique-solutions/verification-identite-kyc/

1.5.2 Informations devant être publiées

Le Prestataire s'engage à publier au minimum les informations suivantes :

- Le présent document, décrivant la Politique et les pratiques du Service ;
- Les CGU du Service ;
- Les points de publication des informations associées aux Services des partenaires.

1.5.3 Délais et fréquences de publication

Les informations liées au Service (évolutions, nouvelle version de la Politique, etc.) sont publiées dès que nécessaire, afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs du Prestataire.

Le point de publication des informations est disponible 24h/7/365(6).

1.5.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est en accès libre en lecture et est consultable ici :

https://www.kipmi.com/

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées du Prestataire. Ces personnes sont définies dans des rôles de confiance et disposent d'un moyen d'authentification forte pour se connecter sur les systèmes de publication.

1.6 Amendement du document

1.6.1 Procédure de mise à jour

Le Prestataire contrôle que tout projet de modification de sa Politique reste conforme aux exigences réglementaires et normatives applicables. Le C2SC intervient toujours en validation des éventuels amendements. Toute demande de changement est donc mise à l'ordre du jour d'un comité futur et la prise de décision est attestée dans le compte rendu correspondant.

Toute proposition d'évolution du Service fait l'objet d'une analyse d'impact afin de déterminer son éventuelle incidence, sur :

- La qualité ou la sécurité du Service ;
- La conformité de l'offre certifiée aux exigences de l'ANSSI ;
- La nécessité de mise à jour des autres documents publiés ;
- Les pratiques internes du Prestataire ou de ses partenaires et fournisseurs.

La présente Politique ne peut être mise à jour concernant les sujets relatifs aux titres d'identité qu'après validation formelle du Référent fraude titre d'identité.

Lors de chaque changement de la procédure de la vérification de visage, une validation formelle du Référent fraude biométrie est exigée.

1.6.2 Circonstances selon lesquelles la Politique doit être changée

Des amendements à la présente Politique peuvent être prévus au cours de la durée de vie du Service, par exemple pour :

- Des corrections mineures (erreurs, précisions supplémentaires…) ;
- Des évolutions ou extensions du Service ;
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique ;
- Des changements d'ordre technique (mise en œuvre, partenaires, fournisseurs, etc…) ;
- Des corrections induites par les audits du Service.

1.6.3 Circonstances selon lesquelles l'OID doit être changé

En cas d'impact majeur, un changement d'OID de Politique est prévu, et l'évolution et son analyse d'impact sont soumises à l'organe de contrôle et à l'organisme d'évaluation de la conformité pour avis ou commentaire.

L'analyse d'impact est étudiée par le C2SC qui valide ou non le lancement d'une évolution. Le cas échéant, la nouvelle Politique sera soumise à l'approbation du C2SC.

1.6.4 Entrée en vigueur de la Politique amendée

La date d'entrée en vigueur de la nouvelle version du document est déterminée par le C2SC dans sa décision de validation tenant compte de la nature et de la complexité des modifications et, le cas échéant, du temps nécessaire aux parties prenantes dans le Service de mettre en œuvre les adaptations y liées.

1.6.5 Mécanisme et période d'information sur les amendements

Une fois l'évolution du Service validée par le C2SC, la nouvelle Politique est communiquée :

- Sans délai au personnel du Prestataire et à toutes les parties prenantes dans la fourniture du Service - par envoi par messagerie. Le délai leur permettant de prendre connaissance des nouvelles dispositions et d'adapter (si besoin) leurs pratiques et procédures, ainsi que la date d'entrée en vigueur, sont explicitement indiqués.
- Au moins 72h (soixante-douze heures) avant sa date d'entrée en vigueur - aux Commanditaires et Utilisateurs - par publication sur le site web : https://www.kipmi.com/

Le Prestataire adresse annuellement à l'organe de contrôle une synthèse de l'ensemble des modifications apportées à la fourniture de son Service.

2. Documents associés

2.1 Conditions générales d'utilisation

Les CGU applicables (et leurs version antérieures) sont disponibles sur le site du Prestataire : https://www.kipmi.com/

2.2 Documents normatifs

Renvoi	Document
[EIDAS]	Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les Services de confiance pour les transactions électroniques au sein du marché intérieur https://www.eur-lex.europa.eu
[ANSSI_PVID]	Prestataire de vérification d'identité à distance – Référentiel d'exigences https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification
[HYGIENE]	Guide d'hygiène informatique https://cyber.gouv.fr/publications/guide-dhygiene-informatique
[NOMADISME]	Recommandations sur le nomadisme numérique https://cyber.gouv.fr/publications/recommandations-sur-le-nomadisme-numerique
[ADMIN_SEC]	Recommandations relatives à l'administration sécurisée des systèmes d'information https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si
[EBIOS_RM]	EBIOS Risk Manager https://cyber.gouv.fr/la-methode-ebios-risk-manager
[PROCESS_QUALIF_SERVICE]	Processus de la qualification d'un Service https://cyber.gouv.fr/procedures-et-formulaires-pour-la-qualification
[RGPD]	https://www.cnil.fr/fr/reglement-europeen-protection-donnees

3. Parties prenantes et obligations

3.1 Prestataire du Service

CheckMi est un Service de la société BE YS TRUSTED SOLUTIONS FRANCE.

Le Prestataire conserve la responsabilité globale de la conformité du Service avec la législation applicable et la présente Politique.

Pour certaines activités le Service peut impliquer des tierces parties. Les relations concernant ces activités seront réglées par des contrats de sous-traitance. Les contrats de sous-traitance doivent définir les droits et les obligations des tierces parties impliquées dans l'activité liée à la fourniture du Service certifié, et les sous-traitants sont obligés de suivre strictement les procédures, conformément à la présente Politique.

3.2 Obligations pour le maintien en condition du Service

Le PVID a recours à la société KIPMI SOFTWARE EAD, une société du Groupe Be Ys, enregistrée en Bulgarie sous le numéro d'enregistrement dans le Registre du Commerce 208651100 , pour garantir le maintien en condition du Service certifié. Elle assure les opérations suivantes :

- L'ensemble des demandes de maintenance évolutive ou corrective exprimées par les équipes internes du Prestataire ;
- L'ensemble des opérations de maintenance techniques indispensables au MCO et à la stratégie de maîtrise des coûts.

Les opérations de maintenance évolutive couvrent l'ensemble des mises à jour et les nouvelles versions de la solution de VID.

3.3 Centre de vérification d'identité a distance

Le PVID a recours à la société Global Remote Services SRL, une société du Groupe Be Ys, enregistrée en Roumanie sous le numéro d'enregistrement 16066508, qui opère un Centre de vérification d'identité à distance. Elle assure la vérification d'identité à distance par des Superviseurs secondaires et des référents fraude.

Dans les CGU, que l'Utilisateur doit valider au lancement de l'application, il est informe que son dossier sera traité en Roumanie.

3.4 Utilisateur

Personne physique utilisant le Service du PVID afin de se faire identifier à distance.

L'Utilisateur doit disposer d'un titre d'identité accepté par le Service et inclus dans la liste des titres d'identité, disponible en Annexe de la présente politique de Service.

3.5 Service métier

Service auprès duquel l'Utilisateur souhaite s'identifier, relevant de la responsabilité du Commanditaire, lequel fait appel au Service de vérification d'identité à distance.

3.6 Référents fraude titre d'identité

Personnels du PVID ou de son sous-traitant disposant de connaissances approfondies sur les éléments de sécurité des titres d'identité et d'une expertise en matière de détection de fraudes aux titres d'identité. Le Prestataire élabore et tient à jour une liste des référents fraude pour chaque titre d'identité accepté.

3.7 Référents fraude

Personnels du PVID ou de son sous-traitant disposant de la capacité à reconnaitre les éléments d'identification du visage d'une personne et d'une expertise en matière de physionomie.

3.8 Chefs d'équipe

Personnels du PVID ou de son sous-traitant en charge de veiller à l'application des Politiques et du règlement intérieur. Au moins un chef d'équipe est présent systématiquement dans les locaux du Centre de vérification d'identité à distance à Bucarest, à chaque instant.

4. Description du Service

4.1 Généralités

Le Service a pour objectif de valider que le titre d'identité présenté par l'Utilisateur est authentique et que l'Utilisateur est le détenteur légitime de ce titre d'identité.

Le Service PVID proposé est délivré en mode SaaS (Software as a Service), pas besoin de télécharger une application sur le terminal de l'Utilisateur. Il fait l'objet de mises à jour régulières qui ont pour finalités d'améliorer la qualité et/ou les fonctionnalités du Service pour l'ensemble de ses Utilisateurs.

L'accès au Service PVID et à l'API est obligatoirement réalisé de manière sécurisée en TLS.

Le verdict est déterminé sur la base des données d'identification (à caractère personnel) acquises et vérifiées par le Service.

Le verdict, ainsi que les attributs d'identité et du titre vérifiés sont ensuite communiqués au Commanditaire.

4.1.1 Langues d'utilisation du Service

Le Service de vérification d'identité supporte au moins les langues suivantes : français et anglais. Au démarrage de l'application, le Service propose à l'Utilisateur la langue qu'il souhaite utiliser.

4.1.2 Parcours de l'utilisateur

Le Commanditaire invite l'Utilisateur à réaliser sa vérification d'identité. Il y a plusieurs façons d'envoyer l'invitation à l'initiative de Commanditaire, soit un lien direct avec une redirection ou non, soit par sms ou courrier électronique….

Si cette invitation est ouverte sur un smartphone, l'Utilisateur commence directement la vérification d'identité.

Si cette invitation est reçue sur une autre chose qu'un smartphone, l'Utilisateur est invité à scanner un QR code depuis son smartphone pour démarrer le processus de la vérification d'identité sur son appareil.

L'étape d'acquisition des données s'effectue depuis le terminal de l'Utilisateur, c'est-à-dire son téléphone mobile (iOS ou Android).

Ensuite l'Utilisateur choisit la langue qu'il souhaite utiliser pendant sa vérification et il est informé des étapes suivantes. Il est invité à accepter l'enregistrement de son visage et les conditions générales d'utilisation. S'il n'accepte pas, l'Utilisateur ne peut pas continuer.

Après l'acceptation, un test de compatibilité et la vérification de qualité de la connexion réseau sont exécutés par l'application.

Si l'appareil est compatible, l'Utilisateur choisit ensuite le pays émetteur du titre d'identité qu'il utilisera et le type du document.

La phase de la vérification du document commence. Lors de cette phase, l'Utilisateur devra présenter la face avant, puis la face arrière (si besoin) de son titre et l'incliner. Il devra ensuite déplacer le document suivant l'information présentée à l'écran de façon aléatoire selon les exigences règlementaires. Durant cette phase une capture du document est réalisée.

La phase de la vérification du visage commence. Lors de cette phase, l'Utilisateur devra placer son visage dans un ovale et suivre les instructions qui seront données. Durant cette phase une capture du visage est réalisée.

Après cette dernière étape d'acquisition, on informe l'Utilisateur que les données acquises sont transférées vers le serveur et le verdict sera rendu prochainement.

Le Service VID s'effectue de manière asynchrone sans interaction humaine.

La vérification de l'identité de l'Utilisateur est réalisée avec l'aide d'un processus faisant appel à l'intelligence artificielle et par suite elle est validée par un Superviseur secondaire humain avec une sollicitation possible du référent fraude.

D'après l'information fournie par le Service et de façon différée, le Superviseur secondaire vérifie que le titre d'identité est authentique et que l'Utilisateur est son détenteur légitime. Le Superviseur secondaire s'assure également du caractère « vivant » de la personne. Le verdict de la vérification d'identité est donné suite à cela. Si le Superviseur secondaire a un doute ou s'il détecte qu'il y une usurpation/fraude, il alerte le référent fraude qui donnera le verdict.

4.1.3 Alternatives au Service VID proposé

CheckMi ne propose pas d'alternative du Service. Tout Utilisateur, ne souhaitant ou ne pouvant pas utiliser le Service de vérification d'identité dans les conditions proposées, peut demander une méthode alternative de vérification d'identité au Commanditaire.

4.2 Titres d'identité

La liste des titres d'identités acceptés par le Service est disponible en annexe. Aucun autre document ne sera accepté. Le Service maintient une liste de Référents fraude titre d'identité compétent pour l'analyse de chacun des titres acceptés.

Seuls les titres non-expirés sont acceptés par le Service.

L'authenticité du titre d'identité est vérifiée par des traitements automatiques, avec une décision finale rendue par un Superviseur secondaire ou un expert de la vérification d'identité (le Référent Fraude). En cas d'invalidité du titre d'identité, et quelle qu'en soit la raison, le verdict de la vérification d'identité est systématiquement « rejeté ».

Les raisons d'invalidité recouvrent, de manière non exhaustive : titre non authentique, titre non original (photocopie par exemple), titre expiré, titre non accepté par le Service, titre endommagé…

Les titres altérés physiquement font l'objet d'un traitement particulier afin de s'assurer que : aucune information n'est indisponible du fait de l'altération ; l'altération résulte d'une usure normale et ne semble pas avoir été provoquée délibérément ; l'altération ne masque pas ou n'empêche pas le contrôle d'éléments de sécurité.

4.2.1 Fraude

Les indicateurs utilisés pour détecter les tentatives d'usurpation d'identité sur la base des scénarios de risques identifiés sont entièrement automatisés et comprennent :

- La détection automatique des incohérences dans le contrôle des données des documents d'identité ;
- La verification avancée des attributs des documents d'identité effectuée par des algorithmes ;
- Les résultats des contrôles automatisés.
- La détection de nouvelles tentatives après une fraude précédemment identifiée ;
- La détection d'édition ou de falsification numérique (deepfakes) ;

Toute suspicion ou détection d'usurpation d'identité identifiée par le système est analysée par un Superviseur Secondaire qui peut faire appel au Référent fraude en cas de doute et qui donnera le verdict final, basé sur le score fourni par le module automatique et l'appréciation de l'humain.

4.2.2 Données d'identification caractérisant l'unicité de l'identité

Les attributs d'identité suivants caractérisent l'unicité de l'identité d'un individu et sont à ce titre transmis au Commanditaire :

- Le nom de naissance ;
- Le nom d'usage (si présent) ;
- Le(s) prénom(s) ;
- Le genre de l'Utilisateur ;
- La date de naissance ;
- Le lieu de naissance ;
- Le type de document ;
- Le pays d'émission ;
- Le numéro unique du titre d'identité ;
- La date d'émission ;
- La date d'expiration ;
- Une photo(s) du titre d'identité extraite de la vidéo du titre ;
- Trois photos du visage de l'Utilisateur extraite de la vidéo du visage.

4.2.3 Liste des données à caractère personnel

Le PVID respecte le principe de minimisation des données personnelles collectées et conservées, et ne traite donc que des données qui sont nécessaires, c'est à dire exigées par la réglementation ou indispensables au parcours d'identification.

Les données à caractère personnel, traitées par le Service pendant la vérification, sont stockées de façon encryptée pendant la durée de conservation du dossier de preuve et sont les suivantes :

4.2.3.1. Données transmises par le Commanditaire :

Le Commanditaire peut nous partager l'adresse électronique de l'Utilisateur dans certains cas d'usage. Mais cette donnée ne participe pas dans le calcul du verdict de la vérification d'identité à distance.

4.2.3.2. Données extraites du titre d'identité :

- La vidéo du titre d'identité ;
- Une photo du titre d'identité extraite de la vidéo du titre ;
- Le numéro unique du titre d'identité ;
- Le nom de naissance de l'utilisateur ;
- Le nom d'usage (si présent) ;
- Le(s) prénoms de l'Utilisateur ;
- La date de naissance de l'Utilisateur ;
- Le lieu de naissance de l'Utilisateur ;
- La nationalité de l'Utilisateur ;
- Le genre de l'Utilisateur ;
- Le numéro personnel d'identité (si présent) ;
- La date d'expiration ;
- La date d'émission ;
- La bande MRZ ;
- Le pays d'émission.

4.2.3.3 Données participant au résultat de la vérification d'identité

Les données faisant partie de la vérification d'identité sont les suivantes :

- Le nom de naissance de l'utilisateur ;
- Le premier prénom de l'Utilisateur ;
- La date de naissance de l'Utilisateur ;
- La date d'expiration ;
- La bande MRZ ;
- La nationalité ;
- Le pays d'émission.

4.2.3.4. Données extraites de la vidéo du visage :

- Trois photos du visage de l'Utilisateur.

4.2.3.5. Données stockées sous forme d'image :

- La photo de la face avant du titre d'identité extraite de la vidéo du titre ;
- La photo du verso du titre d'identité extraite de la vidéo du titre quand elle existe.

4.2.3.6 Données pouvant faire l'objet d'un traitement biometrique

- La photo et la vidéo du visage de l'Utilisateur ;
- Les photos du titre d'identité.

La finalité principale de conservation des données à caractère personnel, relatives aux Utilisateurs et traitées par le Service de vérification, a pour but de constituer un dossier de preuve de la vérification d'identité. Ce dossier de preuve est conservé de façon sécurisée dans un système d'archivage à accès autorisé uniquement en cas de recours légal et à des fins d'audit, ou en cas de réclamation de l'Utilisateur final ou du Commanditaire pour une durée de 6 ans en cas de verdict « succès » ou « échec ».

La vidéo du titre d'identité et la vidéo du visage sont conservées de façon encryptée dans un coffre-fort électronique pour une durée maximum de quatre-vingt-seize heures.

Lorsque la conservation est effectuée au sein du dossier de preuve, l'Utilisateur ne dispose pas de possibilité de rectification ou de suppression du contenu du dossier de preuve ou du résultat de la vérification d'identité.

L'accès aux données traitées de manière automatisée, susceptibles de renseigner sur la nature des vérifications automatisées effectuées par le Service de détection de l'usurpation d'identité, est interdit, sauf dans le cadre de la procédure d'accès au fichier de preuve décrite par la présente politique.

4.3 Recours et réclamations

4.3.1 Voies de soumission

Toute réclamation doit être portée soit au Commanditaire directement, soit au Prestataire à l'adresse suivante :

- Par voie électronique : support@kipmi.com
- Par courrier postal :
  Service Client PVID
  10 Boulevard Haussmann
  75009 PARIS (France)

Les Utilisateurs peuvent adresser toutes les questions concernant le traitement des données personnelles à : dpo@be-ys.com

4.3.2 Gestion des recours et des reclamations

Le demandeur formule et transmet sa demande au Service CheckMi à l'adresse support@kipmi.com en précisant les Nom(s), Prénom(s), le Service métier ayant demandé l'identification, le jour où elle a eu lieu et une description du problème rencontré.

Le Service CheckMi accuse réception de la demande et indique un temps de réponse 10 jours ouvrables maximum pour le traitement de la demande à la suite de l'accuse de réception.

Les demandes portant sur le processus du Service CheckMi, et notamment les étapes et manipulations sont traitées par le fournisseur du Service.

Les demandes portant sur la vérification d'identité d'une personne physique spécifique ne pourront être traitées que par le Service métier. Pour pouvoir traiter la demande, le Service métier doit fournir au fournisseur de Service la référence de la vérification d'identité.

Toutes les réclamations sont consignées dans un outil de traçabilité, création d'un ticket Jira associé avec propre statut. Cet enregistrement permet de générer la statistique des réclamations.

Les Utilisateurs peuvent adresser toutes les questions concernant le traitement des données personnelles à : dpo@be-ys.com

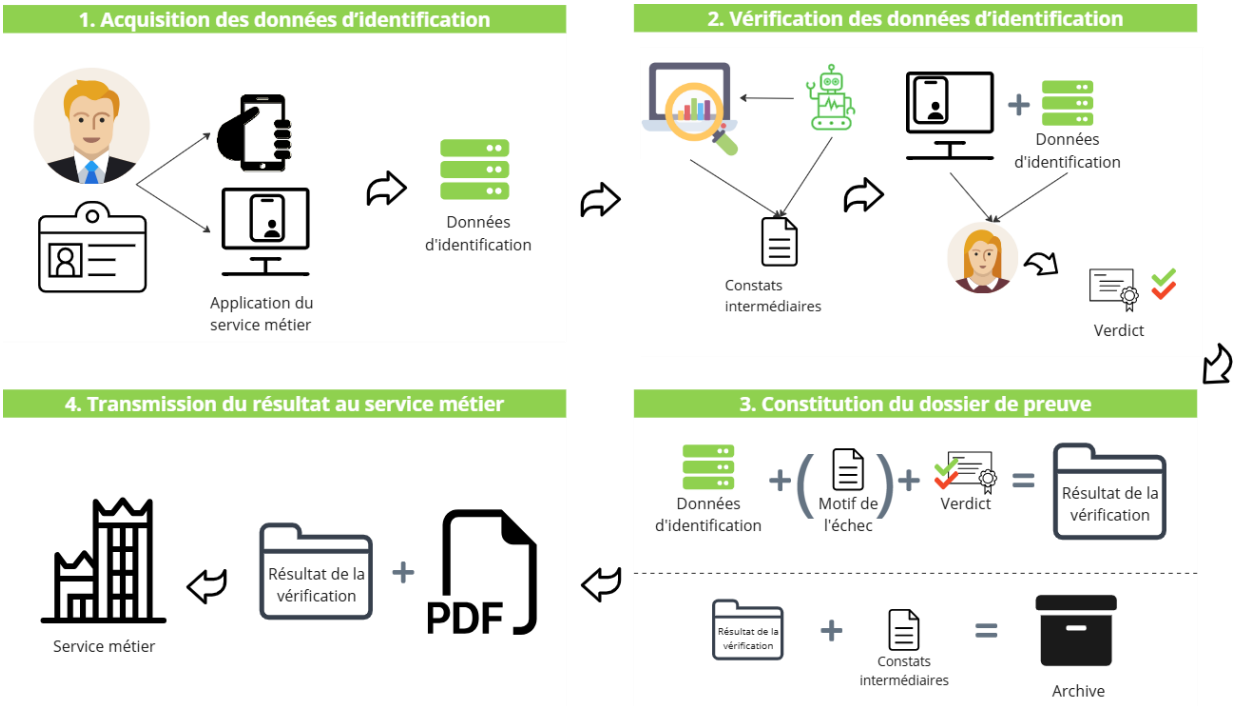
5. Procédure du Service VID

5.1 Activités du Service de vérification d'identité à distance

Le Service de vérification d'identité à distance réalise successivement les quatre étapes suivantes :

1. Étape 1 : Acquisition des données d'identification ;
2. Étape 2 : Vérification des données d'identification ;
3. Étape 3 : Constitution du dossier de preuve
4. Étape 4 : Transmission du résultat de la vérification d'identité à distance.

Le schéma ci-dessous présente une vue fonctionnelle simplifiée du Service.



5.2 Centre de vérification d'identité

Le Centre de vérification d'identité à distance regroupe les Superviseurs secondaires chargés de réaliser les vérifications et de prononcer le verdict. Le Centre de vérification d'identité à distance est opéré par une société du Groupe Be Ys située en Roumanie.

Les horaires de travail du Centre de Vérification sont : de 09:00 à 17:00 CET, du lundi au vendredi (susceptibles d'évoluer).

Si l'Utilisateur fait une demande de vérification en dehors du temps de travail des Superviseurs secondaires, le verdict sera traité le jour de réouverture du centre de contact dans l'ordre chronologique des demandes.

Si pour des raisons inconnues, le Superviseur secondaire ne réussit pas à finaliser la vérification et donner le verdict dans 96h, le Service envoie une statut « échoué ».

5.3 Acquisition des données d'identification

L'acquisition des données est faite en partie de la vidéo du titre d'identité et en partie d'une vidéo du visage de l'Utilisateur.

Lors d'une demande d'un VID, le Commanditaire fournit le prénom, le nom et le courrier électronique (optionnel) de l'Utilisateur.

Le Service n'a pas la possibilité de lire la puce NFC pour les documents qui en sont équipés.

5.4 Exigences techniques liées au terminal de l'utilisateur

Le smartphone de l'Utilisateur doit être équipé d'une caméra frontale et d'une caméra sur l'arrière, ainsi que d'un navigateur web compatible avec le protocole WebRTC. Les navigateurs web compatibles sont les suivants (sans être exhaustifs) :

Type de téléphone	Safari	Chrome	Firefox	Samsung Internet
iOS ≥ 16	✓	✓	✓	-
Android ≥ 8	-	✓	✓	✓

Un enregistrement vidéo du titre d'identité puis du visage de l'Utilisateur sera effectué durant la vérification. Ces vidéos doivent présenter une résolution minimale de 720p (1280 × 720 pixels) à 25 images par secondes et une fluidité suffisante pour une analyse visuelle des éléments de sécurité. Cette vérification est réalisée tout au long du processus de la vérification.

5.4.1 Capture du titre d'identité

Lors de la capture du titre d'identité, le Service CheckMi doit :

- Vérifier la connexion réseau ;
- Vérifier la netteté de la caméra,
- Vérifier l'éclairage du titre et les éventuels reflets (éviter les sources de lumières directes sur le titre) ;
- Vérifier le positionnement du titre au centre de la zone de capture afin qu'il soit entièrement visible ;
- Vérifier que le document correspond au type sélectionné ;
- Incliner le titre d'identité de façon à faire apparaître les marques optiquement variables ;

En cas d'illisibilité ou mauvaise lisibilité persistante de la photographie du titre d'identité, le processus du Service est arrêté et l'Utilisateur est invité à recommencer intégralement le processus d'identification à distance à la demande du Commanditaire.

La capture se déroule de la manière suivante :

- L'Utilisateur sélectionne le titre d'identité qu'il va utiliser pour s'identifier (seuls les titres d'identités acceptés par le PVID figurent parmi les choix proposés) ;
- L'Utilisateur présente le titre d'identité face à sa caméra, une vidéo du titre est ainsi capturée. Si le titre dispose d'un recto et d'un verso cette séquence est exécutée pour chacune des faces du titre.
- La capture du titre intègre un facteur non-prédictible.

Les demandes qui peuvent être formulées par le Service à l'Utilisateur pour une acquisition correcte du titre d'identité sont automatisées et peuvent être les suivantes :

- Indication concernant la position du titre dans le champ de capture
- Indication de luminosité trop faible ou trop importante
- Indication sur la distance du titre par rapport à la camera
- Indication qu'aucun document n'est détecté
- Indication des mouvements à effectuer avec le titre d'identité

5.4.2 Capture du visage de l'utilisateur

Lors de l'étape de capture du visage, le Service CheckMi doit :

- Vérifier la connexion réseau ;
- Vérifier la netteté de la caméra,
- Vérifier l'éclairage du visage et les éventuels surexpositions (éviter les sources de lumières directes sur le visage) ;

Les demandes qui peuvent être formulées par le Service à l'Utilisateur pour une vérification correcte du visage sont automatisées et peuvent être les suivantes :

- Indication concernant la position du visage
- Indication concernant la distance du visage par rapport à la camera
- Indication de luminosité trop faible / contre-jour
- Demande de retrait des accessoires couvrant le visage
- Demande des mouvements à effectuer

5.5 Vérification des données d'identification

Le module automatique contrôle les données récupérées pendant le processus de la vérification : l'authenticité du titre d'identité (attributs et marqueurs du titre d'identité), identification biométrique, caractère vivant de l'Utilisateur.

Aucun traitement, même partiel, ne peut être réalisé sur le terminal de l'Utilisateur et donc ne peut contribuer au verdict « succès » de la vérification d'identité à distance.

5.5.1 Traitement automatique des données d'identification

Le processus de vérification est automatisé. Des algorithmes d'intelligence artificielle effectuent les opérations suivantes pour confirmer que l'utilisateur est le détenteur légitime du document d'identité présenté, ainsi que l'authenticité du titre.

Lors de la vérification des données, le Service contrôle la conformité de la bande MRZ. Si la bande MRZ est invalide, le verdict de la vérification d'identité à distance est systématiquement « échec ».

Chaque résultat de la vérification automatisée du titre d'identité est contrôlé et validé par un vérificateur humain (Superviseur secondaire).

Si le titre est reconnu invalide, le verdict de la vérification d'identité à distance est systématiquement « échec ».

Les données personnelles ne sont conservées que le temps de traitement de la vérification et en aucun cas plus de 96h.

Si l'Etat responsable de l'émission du titre d'identité met à disposition un Service de vérification de validité des titres accessibles par le Service, le Service procèdera systématiquement à la vérification du titre auprès de ce dispositif.

5.5.2 Données biométriques

Le processus de vérification est automatisé. Le Service CheckMi utilise principalement les caractéristiques du visage, les points de repère faciaux et la détection de visage comme données biométriques pour la reconnaissance et la vérification d'identité.

Chaque résultat de la vérification automatisée de la biométrie est contrôlé et validé par un vérificateur humain.

Si la comparaison du visage avec la photo du titre d'identité ne correspond pas, le verdict de la vérification d'identité à distance est systématiquement « échec ».

Les données biométriques ne sont conservées que le temps de traitement de la vérification et en aucun cas plus de 96h.

5.5.3 Contrôle du vivant

Lors du processus de vérification, l'Utilisateur effectue une ou des actions spécifiques non-prédictibles, afin de répondre au besoin de détection du vivant. Il peut être demandé de :

- Tourner la tête ;

- Placer une cible sur des zones du visage ;
- Réaliser des gestes avec la main etc.

Chaque résultat de la vérification automatisée du vivant est contrôlé et validé par un vérificateur humain.

Si le caractère vivant n'est pas identifié, le verdict de la vérification d'identité à distance est systématiquement « échec ».

5.6 Constitution du dossier de preuve

Si la vérification d'identité a pu être réalisée jusqu'au bout, chaque vérification d'identité, quel que soit le verdict « succès » ou « échec » fait l'objet de la création d'un dossier de preuve. Les dossiers de preuve sont chiffrés et automatiquement archivés dans un Système d'Archivage Électronique. Le mode de chiffrement utilise GCM (Galois/Counter Mode) avec AES (Advanced Encryption Standard) à l'aide de clés de 256 bits. Les données de chaque processus VID seront chiffrées avec leur propre clé unique, stockée en toute sécurité dans le module de sécurité matériel (HSM).

L'accès au dossier de preuve encrypté est uniquement accessible à une liste limitée de personnes de confiance chez Be Ys Trusted Solution France. Le décryptage de ce dossier est réalisé par une procédure sécurisée limitée à d'autre groupe réduit de personnes de confiance.

5.6.1 Éléments du dossier de preuve

Les données d'identification

- La vidéo du titre d'identité ;
- Une photographie(s) du titre d'identité ;
- La vidéo du visage de l'Utilisateur ;
- Trois photographies du visage de l'Utilisateur ;
- Le type du titre d'identité (Carte Nationale d'identité, Passeport ou Carte de Séjour) ;
- Le numéro unique du titre d'identité ;
- Le pays émetteur ;
- La date de délivrance du titre d'identité ;
- La date d'expiration du titre d'identité ;
- Le nom de naissance de l'Utilisateur ;
- Le nom d'usage de l'Utilisateur (si présent) ;
- Le(s) prénom(s) de l'Utilisateur ;
- La date de naissance de l'Utilisateur ;
- Le lieu de naissance de l'Utilisateur ;
- La date d'acquisition des données d'identification
- La date de début et de fin de traitement automatique
- La date de début et de fin de traitement manuel
- La date de la vérification de l`authenticité du document auprès des services de l`Etat.

La liste des vérifications réalisées sur les données d'identification, et pour chaque vérification

- La date d'acquisition de chaque donnée d'identification
- La date de la vérification liée à l'activité associée à la vérification ;
- L'activité associée à la vérification, notamment :
  - Vérification de l'authenticité du titre d'identité (liste des marqueurs contrôles avec succès ;
  - Comparaison du visage de l'Utilisateur avec l'heure de traitement associé ;
  - Détection du caractère « vivant » de l'Utilisateur avec l'heure de traitement associé ;
- La nature de la vérification : automatique avec une validation finale manuelle ;
- La version et la configuration le cas échéant des outils ayant réalisé la vérification automatique.
- Le constat intermédiaire rendu par les traitements automatisés.

Toutes les données et actions sont gérées par des systèmes automatisés sans intervention manuelle, et les informations sensibles sont stockées en toute sécurité à des fins d'audit et de vérification de la conformité.

Le verdict (« succès » ou « échec »)

- Les motifs rendus par le Superviseur secondaire ou du Référent Fraude en cas de verdict « échec » ;
- L'identité du Superviseur secondaire ou du Référent Fraude qui a prononcé le verdict ;
- La date à laquelle le verdict a été prononcé par le Superviseur secondaire ou du Référent Fraude ;
- Le pays depuis lequel le Superviseur secondaire ou du Référent Fraude a prononcé le verdict.

Les données constituant le dossier de preuve ont pour finalité de pouvoir résoudre d'éventuels litiges, et en aucun cas d'appliquer un quelconque traitement biométrique.

5.6.2 Conservation du dossier de preuve et sécurité

Une fois la procédure de vérification terminée, les dossiers de preuve sont, de ce fait, automatiquement archivés dans un Système d'Archivage Électronique en respectant la politique d'archivage associée. Cette politique d'archivage sécurise la gestion de l'information de l'établissement en réduisant les risques de perte de données ou les failles de sécurité et détermine les points suivants :

- Les niveaux de Service du Service d'archivage aux Utilisateurs construit sur le SAE ID-Archive (type d'archivage, formats des documents, modalités de communication, durées de conservation, …) interne au Groupe Be Ys ;
- Les fonctionnalités mises en œuvre (fonction de dépôt, de communication, de restitution, …) ;
- Les principes de sécurité à respecter.

La politique « **POL_Politique d'archive id-archive** » de BE YS TRUSTED SOLUTIONS est disponible et consultable afin d'obtenir de plus amples informations.

Les données du Dossier de preuve sont conservées pour une durée maximale de six (6) années à compter de la date de la vérification d'identité.

Lors de la période de conservation susmentionnée, les données du dossier de preuve ne sont soumises à aucun traitement, en particulier biométrique, sauf en cas de requête judiciaire, dans le respect des exigences réglementaires applicables.

5.6.3 Accès au dossier de preuves

L'accès au dossier de preuve ne peut se faire que pour répondre à une réquisition judiciaire ou dans le cadre d'un audit de sécurité, dont l'objectif est de prouver la conformité du dossier de preuve.

Les Utilisateurs peuvent exercer leur droit d'accès aux données à caractère personnel dans le dossier de preuve, toutefois les Utilisateurs ne peuvent pas exercer de droit de rectification sur ce dossier, ni de suppression.

5.7 Transmission du résultat au Commanditaire

Le résultat de la vérification d'identité à distance, quel qu'il soit, « Succès » ou « Échec », est transmis systématiquement au Commanditaire.

Le Commanditaire recevra un rapport de la vérification au format PDF.

5.7.1 Contenu du résultat

Le résultat ne contient que les éléments listés ci-dessous. Il ne contient pas de score issu des vérifications.

Les éléments transmis au Commanditaire, sont les suivants :

Le résultat de la vérification d'identité à distance :

- Le verdict (« succès » ou « échec ») ;

Les données d'identification de l'utilisateur :

- Une photographie du visage de l'Utilisateur ;
- Une ou deux photos de la pièce d'identité ;
- Le type du titre d'identité ;
- Le numéro unique du titre d'identité ;
- Le pays émetteur ;
- La date de délivrance du titre d'identité ;
- La date d'expiration du titre d'identité ;
- Le nom de naissance de l'Utilisateur ;
- Le nom d'usage de l'Utilisateur (si présent) ;
- Le(s) prénom(s) de l'Utilisateur ;
- Le numéro personnel d'identité (si présent) ;
- La date de naissance de l'Utilisateur ;
- Le lieu de naissance de l'Utilisateur ;

- Le contenu de la bande MRZ ;
- La nationalité de l'Utilisateur ;
- Le genre de l'Utilisateur.

Les vidéos du titre d'identité et du visage de l'Utilisateur ne sont en aucune manière transmises au Commanditaire (de façon intégrale ou partielle).

Aucun élément relatif aux vérifications réalisées par le Service autre que le verdict n'est communiqué. La liste de codes externes n'est pas transmise au Commanditaire.

5.7.2 Délai de transmission

Le délai entre le début de l'acquisition des données d'identification de l'Utilisateur et la notification du résultat de la vérification d'identité au Commanditaire ne peut pas dépasser quatre-vingt-seize heures.

5.8 Bulletins opérationnels

Le PVID met en place des bulletins opérationnels et y fait figurer, depuis le dernier bulletin opérationnel :

- Les indicateurs opérationnels du Service ;
- Une revue des réclamations reçues, en cours de traitement et clôturées ;
- Une revue des incidents de sécurité relatifs à la sécurité des systèmes d'information ;
- Une revue des incidents de sécurité notifiés à l'ANSSI ;
- La date de la dernière exécution du plan de test de la capacité effective du Service à détecter des tentatives d'usurpation d'identité ;
- Une revue des éventuelles modifications significatives apportées :
    - Au système d'information du Service de vérification d'identité à distance ;
    - À l'appréciation des risques relatifs à l'usurpation d'identité notamment si la liste des scénarios de risque a été modifiée ;
    - À l'appréciation des risques relatifs à la sécurité des systèmes d'information notamment si la liste des scénarios de risque a été modifiée ;
    - Au plan de traitement des risques ;
    - À la politique de vérification d'identité à distance ;
    - À la déclaration des pratiques de vérification d'identité à distance ;
    - À la politique de sécurité des systèmes d'information ;
    - Au plan de test de la capacité effective du Service à détecter des tentatives d'usurpation d'identité.

Le prestataire transmet les bulletins opérationnels au C2SC tous les mois et doit assurer leur confidentialité.

L'activité du Service est mesurée automatiquement chaque mois afin de vérifier le bon fonctionnement du Service.

6. Protection des données personnelles

6.1 Protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par le Prestataire et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier, la loi Informatique et Libertés et le Règlement Général sur la Protection des Données (RGPD).

6.2 Informations à caractère personnel

Les informations considérées comme personnelles sont détaillées dans section 4.2.3 ci-dessus (« *Liste des données à caractère personnel* »).

6.3 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles transmises au Prestataire par les Utilisateurs du Service ne doivent ni être divulguées, ni transférées à un tiers, sauf dans les cas suivants : décision judiciaire ou autre autorisation légale.

6.4 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Le Prestataire agit dans le respect de la législation et réglementation en vigueur sur le territoire français.

7. Qualité et niveau de service

7.1 Qualité du service

Le Prestataire met en œuvre un processus d'amélioration continue de son Service, notamment en capitalisant sur les incidents et les fraudes détectés.

Le Prestataire définit avec le Commanditaire les indicateurs opérationnels du Service de vérification d'identité à distance. Ces indicateurs sont au moins les suivants :

- Le temps moyen, minimal et maximal d'attente des Utilisateurs ;
- Le nombre de vérifications d'identité à distance réalisées ;
- Le nombre de vérifications selon le verdict (succès ou échec) ;
- Le nombre de vérifications ayant abouti à un verdict « échec », selon le motif ;
- Le nombre de vérifications pour lesquelles une usurpation d'identité était suspectée ou avérée ;
- Le nombre de vérifications « succès » révélées a posteriori comme des usurpations ;
- Le nombre de réclamations reçues, en cours de traitement ou clôturées ;
- Le temps moyen, minimal et maximal de clôture des réclamations.

Le Prestataire maintient un registre indiquant pour chacun de ces indicateurs de quelle manière sont effectuées les mesures et le processus de mesure associé.

7.2 Convention de service

Le Prestataire établit une convention de service avec chacun des Commanditaires souhaitant faire appel au Service. Cette convention contient au moins les éléments exigés par le référentiel PVID de l'ANSSI et peut être annexée à un contrat.

8. Gestion des risques

8.1 Appréciation des risques

Préalablement au lancement du Service, le Prestataire effectue une appréciation des risques conformément à la méthode EBIOS Risk Manager [EBIOS_RM], afin d'identifier et d'évaluer les risques techniques et métiers. L'analyse de risque identifie les systèmes critiques du Service et couvre les risques relatifs à la sécurité des SI et à l'usurpation d'identité.

L'analyse de risques est révisée annuellement et mise à jour en cas de modification significative du Service, notamment en cas de modification de la Politique ou des pratiques relatives à sa fourniture, son hébergement, son infrastructure ou son architecture. Les risques résiduels sont acceptés dans le cadre du processus d'homologation.

8.2 Plan de test de la capacité effective du Service

Le Prestataire établit et maintient un plan de test vérifiant la capacité effective du Service à détecter les tentatives d'usurpation d'identité. Ce plan de test est exécuté régulièrement et ses résultats, notamment les taux de faux négatifs (FRR) et de faux positifs (FAR) pour la vérification de l'authenticité du titre, la comparaison du visage et la détection du vivant, sont communiqués dans les bulletins opérationnels.

9. Protection de l'information et sécurité du système d'information

9.1 Politique de sécurité du système d'information (PSSI)

Le Prestataire dispose d'une PSSI spécifique au Service, approuvée formellement par la direction et communiquée aux employés, sous-traitants, organismes d'évaluation et à l'ANSSI. La PSSI établit un inventaire des actifs du SI, revu régulièrement. Tout changement susceptible d'avoir un impact sur le niveau de sécurité est approuvé par le C2SC. La configuration du SI est régulièrement auditée afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité. La PSSI et l'inventaire des actifs sont revus annuellement.

9.2 Homologation

À la suite de l'analyse de risque, le Prestataire procède à l'homologation du Service. Cette homologation est réalisée préalablement à la fourniture du Service et est renouvelée périodiquement.

9.3 Territorialité du service

L'ensemble des données traitées par le Service est hébergé au sein de l'Union Européenne. Les traitements manuels sont réalisés depuis le Centre de vérification d'identité à distance situé en Roumanie (UE). Les serveurs du Service sont hébergés dans des centres de données situés dans l'UE.

9.4 Niveau de sécurité

Le Prestataire s'engage à maintenir un niveau de sécurité conforme aux exigences du référentiel PVID et aux recommandations de l'ANSSI en matière d'hygiène informatique [HYGIENE].

9.5 Contrôle d'accès au SI

L'accès au système d'information du Service est strictement contrôlé. Les accès sont basés sur le principe du moindre privilège et protégés par une authentification forte. Les droits d'accès sont revus régulièrement.

9.6 Sécurité physique et environnementale

Les locaux abritant les équipements du Service sont protégés par des mesures de sécurité physique adaptées. Les accès physiques sont contrôlés, tracés et réservés aux personnes habilitées. Le Centre de vérification d'identité à distance en Roumanie est soumis aux mêmes exigences de sécurité physique.

9.7 Journalisation

Le Service journalise l'ensemble des événements liés à la sécurité et à l'exploitation. Les événements enregistrés comprennent au minimum :

- Les tentatives d'accès au Service (réussies et échouées) ;
- Les opérations d'administration du Service ;
- Les événements liés au cycle de vie des vérifications d'identité ;
- Les incidents de sécurité ;
- Les modifications de la configuration du Service.

Les journaux sont conservés un an minimum, protégés en intégrité et confidentialité, et sauvegardés régulièrement.

9.8 Sauvegardes

Le Prestataire met en œuvre une politique de sauvegarde couvrant l'ensemble des éléments nécessaires au fonctionnement du Service. Les sauvegardes sont testées régulièrement afin de vérifier leur exploitabilité.

9.9 Cloisonnement du système d'information

Le système d'information supportant le Service est cloisonné des autres systèmes d'information du Prestataire et de ses sous-traitants. Ce cloisonnement est assuré au niveau réseau et système.

9.10 Administration et exploitation du Service

L'administration du Service est réalisée conformément aux recommandations de l'ANSSI relatives à l'administration sécurisée des systèmes d'information [ADMIN_SEC]. Les accès d'administration sont protégés par une authentification forte et tracés.

9.11 Interconnexions avec le service métier

Les échanges entre le Service et les services métier des Commanditaires sont sécurisés par le protocole TLS. Les Commanditaires accèdent au Service via une API sécurisée dont les modalités d'authentification sont définies dans la convention de service.

9.12 Développement et sécurité des logiciels

Le Prestataire met en œuvre un processus de développement sécurisé incluant des revues de code, des tests de sécurité et une gestion des vulnérabilités. Toute mise en production fait l'objet d'un processus de validation intégrant des tests de non-régression.

9.13 Gestion des incidents

Le Prestataire dispose d'une procédure de gestion des incidents de sécurité. Les incidents de sécurité relatifs au Service sont notifiés à l'ANSSI dans les conditions prévues par le référentiel PVID. Le Prestataire tient un registre des incidents et des actions correctives associées.

9.14 Sécurité réseau et tests d'intrusion

Le Prestataire met en œuvre des mesures de sécurité réseau conformes aux bonnes pratiques, incluant le filtrage du trafic, la détection d'intrusion et des tests d'intrusion réguliers réalisés par un prestataire qualifié PASSI.

9.15 Continuité d'activité

Le Prestataire dispose d'un plan de continuité d'activité et d'un plan de reprise d'activité permettant d'assurer la disponibilité du Service en cas de sinistre. Ces plans sont testés régulièrement.

10. Organisation du prestataire et gouvernance

10.1 Rôles de confiance

Le Prestataire définit des rôles de confiance pour les personnes intervenant dans la fourniture du Service. Ces rôles incluent au minimum : les administrateurs systèmes, les Superviseurs secondaires (opérateurs), les Référents fraude titre d'identité, les Référents fraude biométrie, les chefs d'équipe et l'officier de sécurité. Les attributions et responsabilités de chaque rôle sont formalisées.

10.2 Séparation des tâches

Le Prestataire met en œuvre une séparation des tâches afin qu'aucune personne ne puisse, seule, compromettre l'intégrité du Service. En particulier, les fonctions d'administration du SI et de vérification d'identité sont assurées par des personnes distinctes.

10.3 Ressources humaines

10.3.1 Vérification des antécédents

Le Prestataire vérifie les antécédents des personnes appelées à occuper des rôles de confiance, conformément à la législation applicable.

10.3.2 Formation initiale et continue

Le personnel occupant des rôles de confiance reçoit une formation initiale adaptée à ses fonctions, notamment en matière de détection de fraude documentaire et biométrique. Des formations continues sont dispensées régulièrement afin de maintenir le niveau de compétence requis face à l'évolution des menaces.

10.3.3 Charte d'éthique

Tout personnel intervenant dans la fourniture du Service signe une charte d'éthique couvrant les obligations de confidentialité, les règles de déontologie et les sanctions applicables en cas de manquement.

10.3.4 Sanctions

Des sanctions disciplinaires sont prévues en cas d'actions non autorisées ou de non-respect des règles et procédures établies dans le cadre du Service.

10.4 Audit de conformité

Le Service fait l'objet d'audits de conformité réguliers conduits par des organismes d'évaluation habilités par l'ANSSI. Les résultats des audits font l'objet d'un plan d'actions correctives validé par le C2SC.

11. Autres problématiques métiers et légales

11.1 Responsabilité financière et assurances

Le Prestataire dispose d'une assurance de responsabilité civile professionnelle couvrant les risques liés à la fourniture du Service de vérification d'identité à distance.

11.2 Confidentialité des données professionnelles

Les informations confidentielles comprennent l'ensemble des données techniques, opérationnelles et organisationnelles relatives au Service, à l'exception des informations rendues publiques par la présente Politique. Le Prestataire et ses sous-traitants sont tenus de respecter la confidentialité de ces informations.

11.3 Obligations des Utilisateurs

L'Utilisateur s'engage à présenter un titre d'identité authentique dont il est le détenteur légitime, à réaliser les étapes du parcours de vérification de bonne foi et à ne pas tenter de contourner les mécanismes de sécurité du Service. Toute tentative d'usurpation d'identité est susceptible de poursuites judiciaires.

11.4 Fin d'activité

En cas de cessation d'activité du Prestataire, celui-ci s'engage à assurer le transfert des dossiers de preuve vers une entité désignée, en accord avec les Commanditaires et dans le respect de la réglementation applicable. L'ANSSI est informée de toute cessation d'activité.

11.5 Conformité aux législations et réglementations

Le Prestataire s'engage à se conformer à l'ensemble des législations et réglementations applicables, notamment le Règlement eIDAS, le RGPD, la directive LCB-FT et le Code Monétaire et Financier, dans le cadre de la fourniture du Service.

11.6 Force majeure

Le Prestataire ne saurait être tenu responsable de l'inexécution de ses obligations en cas de force majeure telle que définie par la législation française. Le Prestataire s'engage toutefois à informer les Commanditaires et les Utilisateurs dans les meilleurs délais et à mettre en œuvre les mesures nécessaires pour réduire l'impact d'un tel événement.

11.7 Résolution des conflits

Tout litige relatif à la fourniture du Service sera soumis au droit français. En cas de différend, les parties s'efforceront de trouver une solution amiable. À défaut, le litige sera porté devant les juridictions compétentes.

12. Annexes

12.1 Liste des titres acceptés par le Service

Type de document d'identité	**Pays**	**Références**	**Commentaires**
Carte nationale d'identité (nouvelle)	France	FRA-BO-03001	Avec prise en charge NFC, actuellement illisible
Carte nationale d'identité (ancienne sans NFC)	France	FRA-BO-02002	Pas de prise en charge NFC
Passeport	France	FRA-AO-03004	Avec prise en charge NFC
Carte de résident	France	FRA-HO-12001	Pas de prise en charge NFC
Carte nationale d'identité (ancienne sans NFC)	Bulgarie	BGR-BO-02001	Pas de prise en charge NFC
Passeport	Bulgarie	BGR-AO-02001	Avec prise en charge NFC
Carte de résident	Bulgarie	BGR-HO-01001	Pas de prise en charge NFC
Carte nationale d'identité (nouvelle)	Roumanie	ROU-BO-05001	Avec prise en charge NFC
Passeport	Roumanie	ROU-AO-03001	Avec prise en charge NFC
Carte de résident	Roumanie	ROU-HO-04003 ROU-HO-04002	NFC support