RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires de vérification d'identité à distance

Référentiel d'exigences

Version 1.1 du 1er mars 2021

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
19/11/2020	1.0	*Version préliminaire pour appel à commentaires.*	ANSSI
01/03/2021	1.1	*Première version applicable*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

commentaires-pvid@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

La transformation numérique de la société a créé le besoin de pouvoir identifier, à distance, des personnes souhaitant accéder à des services publics ou privés en ligne, lorsqu'elles ne disposent pas d'une identité numérique reconnue par ces services. Afin de garantir la fiabilité de ces processus, la réglementation prévoit que l'Agence nationale de la sécurité des systèmes d'information (ANSSI), avec l'appui du ministère de l'Intérieur, puisse évaluer des services de vérification d'identité à distance.

Un service de vérification d'identité à distance[1] possède ainsi la même finalité qu'une vérification d'identité en présentiel, à savoir vérifier que le titre d'identité[1] présenté par l'utilisateur[1] est authentique et que l'utilisateur est le légitime détenteur du titre d'identité. Le principal objectif visé par des personnes malveillantes contre un service de vérification d'identité à distance est identique à celui contre une vérification d'identité en présentiel, à savoir l'usurpation ou l'altération d'identité.

Un service de vérification d'identité à distance est exposé aux mêmes risques qu'une vérification d'identité en présentiel mais, de par sa nature, est également exposé à des scénarios de risque spécifiques.

Le présent référentiel contient les exigences applicables aux services de vérification d'identité à distance afin qu'ils offrent un niveau de garantie en fonction des risques et des profils des attaquants. Les niveaux de garantie visés par le présent référentiel attestent d'une vérification d'identité à distance répondant aux objectifs de sécurité définis par le règlement européen [EIDAS] pour :

- le niveau de garantie substantiel[1], qui vise à réduire substantiellement le risque d'usurpation ou d'altération de l'identité, le service doit garantir l'équivalence en termes de fiabilité avec un face à face physique réalisé dans le cadre de l'accès à un service public ou privé nécessitant une preuve d'identité (par exemple, par une personne formée de manière générale à la comparaison de visages et à la détection titres d'identité altérés ou falsifiés mais ne disposant pas d'outillage élaboré). Le service doit résister à un attaquant disposant d'un potentiel d'attaque modéré[1] ;
- le niveau de garantie élevé[1], qui vise à empêcher le risque d'usurpation ou d'altération de l'identité, le service doit garantir l'équivalence en termes de fiabilité avec un face à face physique réalisé dans le cadre de la délivrance d'un titre d'identité (par exemple réalisé par une personne formée à la lutte contre la fraude identitaire et disposant d'un outillage spécifique permettant de confirmer l'authenticité des titres d'identité et formée à la comparaison des visages). Le service doit résister à un attaquant disposant d'un potentiel d'attaque élevé[1].

Le présent référentiel n'impose aucune architecture pour le système d'information du service de vérification à distance, plusieurs implémentations sont donc envisageables. Le présent référentiel ne crée pas non plus de restriction relative à la typologie ou à l'organisation des prestataires de vérification d'identité à distance (qui peuvent être des organismes publics ou privés, ayant recours à de la sous-traitance ou non sur tout ou partie de leurs activités) ni à l'imbrication entre le prestataire de vérification d'identité à distance et le commanditaire (qui peut être totalement externe ou opérer un service de vérification à distance en interne pour ses propres besoins).

I.1.2. Objet du document

Ce document constitue le référentiel d'exigences (ci-après dénommé « le référentiel ») applicable à un prestataire de vérification d'identité à distance, ci-après dénommé « le prestataire ».

Ce document ne formalise pas d'exigences relatives au commanditaire du service de vérification d'identité à distance, ci-après dénommé « le commanditaire ».

[1] Voir définitions au chapitre I.3.2.

Ce référentiel a vocation à être utilisé dans différents cadres réglementaires, selon les modalités décrites au chapitre III.

I.1.3. Structure du document

Le chapitre I correspond à l'introduction du référentiel.

Le chapitre II décrit les activités visées par le référentiel.

Le chapitre III présente les modalités d'évaluation et de certification des prestataires attestant de leur conformité aux exigences du référentiel.

Le chapitre IV présente les exigences que les prestataires doivent respecter pour être conformes au référentiel.

L'Annexe 1 présente les références des textes législatifs, réglementaires, normatifs et autres mentionnés dans le référentiel.

L'Annexe 2 présente les missions et compétences attendues du personnel du prestataire.

L'Annexe 3 présente les recommandations aux commanditaires de prestations de vérification d'identité à distance.

L'Annexe 4 présente les titres d'identité que peut accepter un prestataire conforme au référentiel.

I.1.4. Champ d'application du document

Le référentiel formule des exigences applicables aux prestataires de vérification d'identité à distance, que ces services soient asynchrones[2], synchrones avec interaction humaine[2], synchrones sans interaction humaine[2], internes[2] ou externes[2].

Le référentiel ne traite pas de :

- la vérification d'identité à distance de personnes morales ou du lien entre des personnes physiques et des personnes morales ;
- la vérification d'identité à distance sur la base d'autres mécanismes que la comparaison de visage ;
- la vérification de données complémentaires[2] acquises par le service de vérification d'identité à distance.

Le référentiel n'exclut ni l'application de la législation et de la réglementation en matière de protection des données à caractère personnel, notamment [RGPD], ni l'application des règles générales imposées aux prestataires en leur qualité de professionnels et notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

I.1.5. Mise à jour du document

L'opportunité de la mise à jour du référentiel est évaluée par l'ANSSI et peut être le fait d'une évolution du cadre législatif, réglementaire ou normatif, de l'état de l'art, de l'évaluation de la menace ou du processus d'évaluation des prestataires de vérification d'identité à distance.

L'ANSSI précise la date d'effet de chaque mise à jour et les modalités de transition le cas échéant.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires de vérification d'identité à distance – Référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

[2] Voir définitions au chapitre I.3.2.

I.3. Acronymes et définitions

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
OID	*Object Identifier*
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PRADO	*Public Register of Authentic Travel and Identity Documents Online*[3] - Registre public en ligne de documents authentiques d'identité et de voyage
SI	Système d'information
SSI	Sécurité des systèmes d'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)

I.3.2. Définitions

Les définitions ci-dessous s'appliquent au présent référentiel. Certaines d'entre elles s'appuient 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 composants du système d'information du service de vérification d'identité à distance.

Attributs d'identité – sous-ensemble des données d'identification transmis par le service de vérification d'identité à distance au service métier.

Commanditaire – entité responsable d'un service métier ayant recours à un service de vérification d'identité à distance.

Composant de sécurité – composant électronique d'un titre d'identité, utilisé comme support de stockage sécurisé des données d'état civil ainsi que de la photographie du légitime détenteur de ce titre. L'accès aux informations contenues dans le composant de sécurité d'un titre d'identité peut faire l'objet de restrictions dans le droit national des États.

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

Consentement – toute manifestation de volonté, libre, spécifique, éclairée 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.

Constat intermédiaire de la vérification d'identité à distance – information générée par le service de vérification d'identité à distance dans le cadre d'analyses réalisées par des traitements automatiques ou par

[3] Registre public en ligne des documents authentiques d'identité et de voyage.

des opérateurs, et nécessaires à l'élaboration du verdict de la vérification d'identité à distance. Plusieurs constats intermédiaires peuvent contribuer à un même verdict.

Convention de service – accord écrit ou contrat entre un prestataire de vérification d'identité à distance et un commanditaire pour la réalisation de la prestation. Dans le cas où le prestataire est un organisme privé, la convention de service inclut le contrat.

Déclaration des pratiques de vérification d'identité à distance – ensemble de pratiques (organisation, procédures opérationnelles, moyens techniques et humains, etc.) que le prestataire de vérification d'identité à distance applique dans le cadre de la fourniture de sa prestation et en conformité avec la politique de vérification d'identité à distance qu'il s'est engagé à respecter. La déclaration des pratiques de vérification d'identité à distance est confidentielle et n'est mise à disposition que des seules personnes ayant le besoin d'en connaître.

Détection du vivant – la détection du caractère « vivant » de l'utilisateur vise à authentifier la vidéo du visage de l'utilisateur, pour vérifier que celui-ci n'a pas fait l'objet d'altération physique ou numérique.

Données d'identification – ensemble de données à caractère personnel acquises et vérifiées par le service afin de vérifier l'identité d'une personne physique. Dans le cadre du présent référentiel les données d'identification peuvent être la vidéo du visage de l'utilisateur, la vidéo du titre d'identité présenté par l'utilisateur, ou les données relatives à l'utilisateur (dont la photographie du visage de l'utilisateur) stockées dans le composant de sécurité du titre d'identité.

Données à caractère personnel – toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une « personne physique identifiable » une personne physique 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 – les 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 complémentaires – données acquises par le service de vérification d'identité à distance et transmises au service métier dans le résultat de vérification d'identité à distance mais sur lesquelles aucune vérification n'est réalisée par le service dans le cadre du référentiel. Les données complémentaires n'entrent en aucun cas dans le verdict de la vérification d'identité à distance. L'acquisition par le service de vérification d'identité à distance de ces données complémentaires et leur transmission au service métier doivent s'effectuer dans le respect de la réglementation applicable, et sont en général demandées par le commanditaire pour satisfaire à des exigences réglementaires.

Dossier de preuve – élément conservé par le prestataire rassemblant les informations pertinentes à produire pour la résolution de litiges, ou en cas d'enquête et notamment afin de fournir des preuves en justice. Le présent référentiel spécifie les données minimales à conserver. Les données contenues dans le dossier de preuve ne sont pas conservées à des fins de traitement biométrique.

État de l'art – ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information ou à la vérification d'identité publiquement accessibles, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine législatif, réglementaire ou normatif.

Légitime détenteur du titre d'identité – personne à qui le titre d'identité a été émis par le pays émetteur, et dont l'identité est représentée par ce titre d'identité.

Motif de l'échec – cause d'un verdict « échec » de la vérification d'identité à distance. Le motif de l'échec est transmis par le service de vérification d'identité à distance au service métier ou à l'utilisateur et permet notamment de faire la distinction entre un échec relatif à une suspicion de fraude et un échec pour des

raisons techniques (résolution de la caméra du terminal insuffisante, luminosité insuffisante, problème de mise au point, etc.). En cas de suspicion de fraude, le motif ne comporte aucune information sur les vérifications réalisées ou sur le type de fraude suspecté.

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

Niveau de garantie élevé – ce niveau vise à empêcher le risque d'usurpation ou d'altération de l'identité. Un service de vérification d'identité à distance est dit de niveau de garantie élevé lorsqu'il est démontré qu'il répond aux exigences du référentiel pour le niveau élevé.

Niveau de garantie substantiel – ce niveau vise à réduire substantiellement le risque d'usurpation ou d'altération de l'identité. Un service de vérification d'identité à distance est dit de niveau de garantie substantiel lorsqu'il est démontré qu'il répond aux exigences du référentiel pour le niveau substantiel.

Opérateur – personnel du service de vérification d'identité à distance en charge de vérifier l'identité des utilisateurs, de prononcer le verdit « succès » ou « échec » de la vérification d'identité à distance et d'alerter un référent fraude en cas de suspicion d'usurpation d'identité.

Politique de vérification d'identité à distance – ensemble de règles, qui dispose d'une référence unique identifiée par un OID, définissant les exigences auxquelles un prestataire de service de vérification d'identité à distance se conforme dans la mise en place et la fourniture de sa prestation. Une politique de vérification d'identité à distance peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les utilisateurs et les commanditaires. La politique de vérification d'identité à distance est mise à disposition des utilisateurs.

Potentiel d'attaque – mesure de l'effort à fournir 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 document [CC_CEM] fournit des indications relatives au calcul d'un potentiel d'attaque élevé (« *high* ») ou modéré (« *moderate* »).

Prestataire – personne morale qui fournit un service de vérification d'identité à distance.

Prestation – fourniture du service de vérification d'identité à distance à un commanditaire, dans le cadre de la convention de service établie entre le prestataire et le commanditaire.

Référent fraude Titre d'identité – personnel du service de vérification d'identité à distance 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.

Référent fraude Biométrie – personnel du service de vérification d'identité à distance disposant de connaissances approfondies en biométrie et d'une expertise en matière de détection de fraudes biométriques.

Résultat de la vérification d'identité à distance – ensemble d'informations transmis par le service de vérification d'identité à distance au service métier et comprenant le verdict (succès ou échec) de la vérification d'identité à distance, le motif de l'échec le cas échéant, les attributs d'identité relatifs aux utilisateurs requis par le service métier et vérifiés par le prestataire, ainsi que les éventuelles données complémentaires requises par le service métier.

Sous-traitance – opération par laquelle le prestataire confie sous sa responsabilité à une entité tout ou partie de l'exécution de la convention de service (et le cas échéant du contrat) conclue avec le commanditaire.

Service de vérification d'identité à distance – service objet du présent référentiel, chargé de l'acquisition et la vérification les données d'identification des utilisateurs afin de les identifier, de la constitution du dossier de preuve et de la transmission du résultat de la vérification d'identité à distance au service métier.

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 réalisée de manière différée par rapport à 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 de vérification d'identité à distance hybride – un service de vérification d'identité à distance est dit hybride lorsque le verdit « succès » du résultat de la vérification d'identité à distance ne peut être prononcé que par un opérateur après que ce dernier a validé les résultats des vérifications réalisées par des traitements automatisés et réalisé sa propre vérification des données d'identification.

Service de vérification d'identité à distance interne – un service de vérification d'identité à distance est dit interne dans les deux cas suivants : s'il est offert exclusivement à des services métier ayant un lien juridique au sens des articles L. 233-l et suivants du Code de commerce avec une même personne morale et opéré par un prestataire ayant lui aussi un lien juridique de même nature avec la même personne morale ; s'il est offert à des services métier appartenant à la même autorité administrative, au sens de l'article I-1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et opéré par un prestataire appartenant à la même autorité administrative.

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 qu'il permet des interactions entre l'utilisateur et l'opérateur lors de la phase d'acquisition ou de 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 lors de 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 qu'il ne permet aucune interaction entre l'utilisateur et l'opérateur lors des phases d'acquisition et de vérification des données d'identification. Le service peut néanmoins mettre en œuvre des interactions automatisées avec l'utilisateur.

Service métier – service auprès duquel l'utilisateur souhaite s'identifier, relevant de la responsabilité du commanditaire, faisant appel au service de vérification d'identité à distance.

Terminal – matériel informatique (téléphone portable, tablette, ordinateur, etc.) utilisé pour acquérir les données d'identification de l'utilisateur. Le terminal peut être celui de l'utilisateur, celui du prestataire ou celui du commanditaire. L'acquisition des données d'identification de l'utilisateur au travers du 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 à l'aide de procédés automatisés ou non 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.

Titre d'identité – document officiel certifiant l'identité d'une personne. Sont acceptés dans le cadre du présent référentiel les titres d'identité référencés à l'Annexe 4 du présent référentiel.

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

Usurpation d'identité – action consistant à utiliser frauduleusement les données d'identification d'un tiers. Dans le cadre de ce référentiel, la notion d'usurpation d'identité englobe également l'altération de l'identité, consistant à utiliser des données d'identification frauduleuses qui n'appartiennent pas à une personne existante.

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

II. Description générale du service de vérification d'identité à distance

II.1. Activités du service de vérification d'identité à distance

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

- l'acquisition des données d'identification, décrite au chapitre II.1.1 ;
- la vérification des données d'identification, décrite au chapitre II.1.2 ;
- la constitution du dossier de preuve, décrite au chapitre II.1.3 ;
- la transmission du résultat de la vérification d'identité à distance, décrite au chapitre II.1.4.

Le schéma ci-dessous présente une vue fonctionnelle simplifiée d'un service de vérification d'identité à distance (asynchrone dans cet exemple) et illustre les quatre étapes successives du service de vérification d'identité à distance.

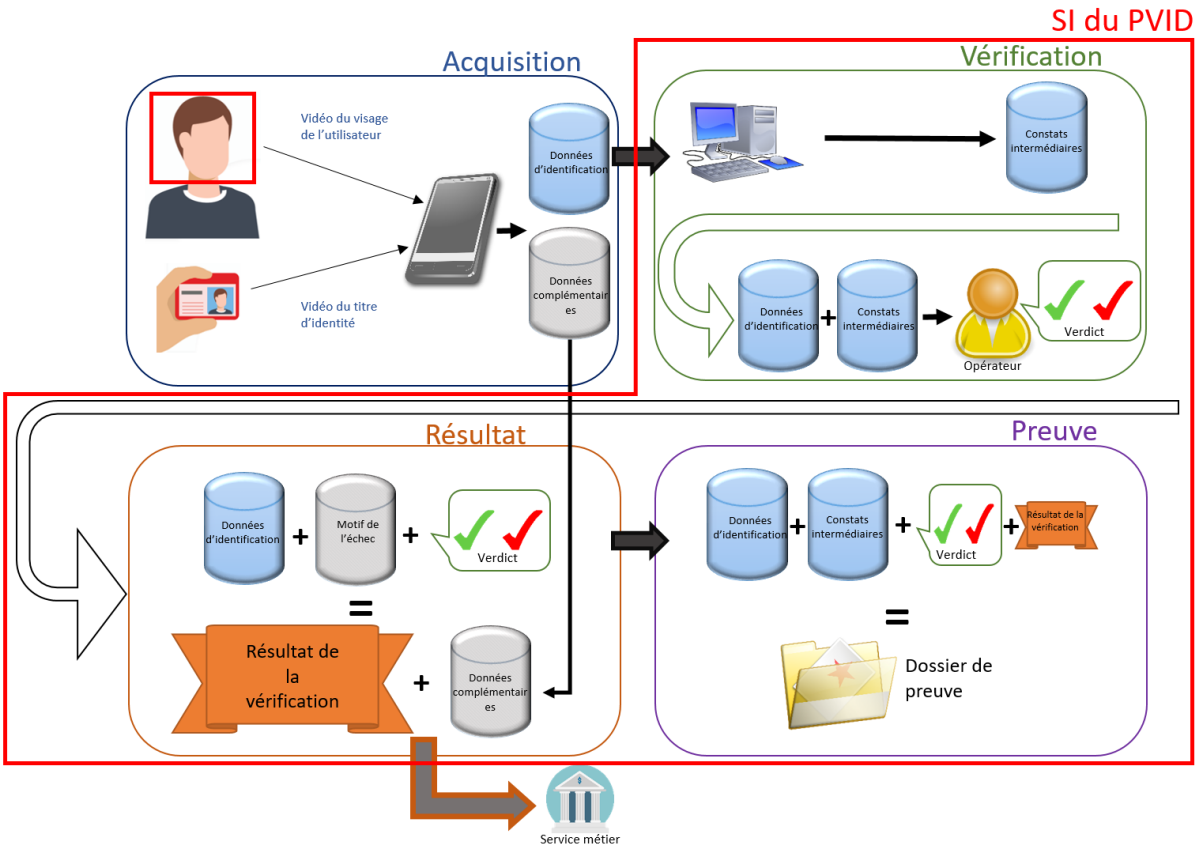

Figure 1: Vue fonctionnelle simplifiée d'un service de vérification d'identité à distance

II.1.1. Acquisition des données d'identification

Cette étape consiste à acquérir les données d'identification relatives à l'utilisateur, à savoir :

- une vidéo du visage de l'utilisateur ;
- [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] une vidéo du titre d'identité présenté par l'utilisateur ;

- [lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] les données d'identification relatives à l'utilisateur (dont la photographie du visage de l'utilisateur) stockées dans le composant de sécurité du titre d'identité présenté par l'utilisateur.

Les acquisitions des différentes données d'identification peuvent être réalisées simultanément ou successivement, dans un ordre indifférent. Ainsi, les acquisitions des vidéos du visage de l'utilisateur et du titre d'identité présenté par l'utilisateur peuvent être réalisées de deux manières différentes :

- acquisition d'une vidéo unique dans laquelle l'utilisateur présente son visage et son titre d'identité ;
- acquisition de deux vidéos distinctes : une vidéo du titre d'identité de l'utilisateur et une vidéo du visage de l'utilisateur. La vidéo du titre d'identité peut être acquise dans un premier temps et la vidéo du visage de l'utilisateur dans un second temps, ou inversement.

Le terminal utilisé pour acquérir les données d'identification peut être celui de l'utilisateur, celui du prestataire ou celui du commanditaire.

Le service de vérification d'identité à distance protège en confidentialité et en intégrité les données d'identification de l'utilisateur lorsqu'elles transitent entre le terminal et le service de vérification d'identité à distance.

II.1.2. Vérification des données d'identification

Sur la base des données d'identification acquises lors de l'étape précédente, cette étape consiste à vérifier à l'aide de traitements, à la fois automatisés et humains, que le titre d'identité présenté par l'utilisateur est authentique et que l'utilisateur est le légitime détenteur du titre d'identité.

La vérification du fait que l'utilisateur est le légitime détenteur du titre d'identité comprend :

- une vérification de l'authenticité du titre d'identité présenté ;
- une détection du caractère « vivant » de l'utilisateur représenté dans la vidéo ;
- une comparaison du visage de l'utilisateur extrait de la vidéo de l'utilisateur avec :
    - [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] une photographie du visage de l'utilisateur extraite de la vidéo du titre d'identité ;
    - [lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] la photographie de l'utilisateur extraite du composant de sécurité du titre d'identité.

Ces vérifications donnent lieu à des constats intermédiaires et peuvent être réalisées simultanément ou successivement, dans un ordre indifférent.

II.1.3. Constitution du dossier de preuve

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

Le service de vérification d'identité à distance protège en confidentialité et en intégrité le dossier de preuve.

II.1.4. Transmission du résultat de la vérification d'identité

Cette étape consiste à transmettre au service métier le résultat comprenant le verdict (échec ou succès) de la vérification d'identité, le motif de l'échec le cas échéant, les attributs d'identité relatifs à l'utilisateur vérifiés par le prestataire, ainsi que le cas échéant les données complémentaires demandées par le service métier dont le recueil n'est pas encadré par le présent référentiel.

Les éventuelles données complémentaires doivent être recueillies et transmises dans le respect de la réglementation applicable.

Le service de vérification d'identité à distance protège en confidentialité et en intégrité le résultat de la vérification d'identité de l'utilisateur lorsqu'il transite entre le service de vérification d'identité à distance et le service métier.

III. Evaluation des prestataires de vérification d'identité à distance

III.1. Modalités d'évaluation

Le référentiel contient des exigences et des recommandations à destination des prestataires de vérification d'identité à distance.

Les exigences doivent être respectées par le prestataire pour que le service puisse être certifié conforme au présent référentiel.

Les recommandations sont données à titre de bonnes pratiques et ne font pas l'objet d'évaluation.

Sauf indication contraire, les exigences et recommandations sont les mêmes pour les systèmes de vérification d'identité à distance, qu'ils soient asynchrones, synchrones avec interaction humaine, synchrones sans interaction humaine, internes ou externes, mis en œuvre dans le cadre d'un service de confiance, d'un moyen d'identification électronique ou d'un service d'entrée en relation d'affaires à distance, que le terminal utilisé pour l'acquisition des données d'identification soit celui de l'utilisateur, celui du prestataire ou celui du commanditaire.

Les exigences sont applicables quel que soit le niveau de garantie visé, aux exceptions suivantes :

- les exigences et recommandations identifiées par le préfixe [SUBSTANTIEL] ne sont applicables que pour le niveau de garantie substantiel ;
- les exigences et recommandations identifiées par le préfixe [ELEVE] ne sont applicables que pour le niveau de garantie élevé.

Si le prestataire sous-traite une partie des activités du service de vérification d'identité à distance, alors les sous-traitants mettant en œuvre tout ou partie des moyens humains, techniques et organisationnels nécessaires au respect des exigences de ce référentiel sont évalués pour vérifier qu'ils respectent les exigences qui leur incombent.

Le référentiel formule également des recommandations aux commanditaires dans l'Annexe 3. Ces recommandations ne font pas l'objet d'évaluation.

III.2. Cadres réglementaires applicables

Le présent référentiel est applicable dans le cadre de :

- **la certification au titre du [DECRET_2020-118] des services d'entrée en relation d'affaires à distance** mis en œuvre par des organismes assujettis à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Dans ce cas, la certification est octroyée par l'ANSSI, conformément au processus [PROCESS_CERTIF_SERVICE], pour une durée maximale de deux ans.
- **la qualification des services de confiance au titre du règlement [EIDAS] lorsque ces derniers recourent à une vérification d'identité à distance.** Dans ce cas, la qualification est octroyée par l'ANSSI, conformément au processus [PROCESS_QUALIF_SERVICE], pour une durée maximale de deux ans. Le recours à un service de vérification d'identité à distance certifié au titre du [DECRET_2020-118] permet d'apporter une présomption de conformité aux exigences relatives à la vérification d'identité à distance pour un niveau de garantie donné.
- **l'évaluation de la conformité des moyens d'identification électronique au titre du règlement [EIDAS] et leur certification au titre de l'article L.102 du [CPCE], pour les niveaux de garantie substantiel et élevé, lorsque ces derniers recourent à une vérification d'identité à distance**. Dans ce cas, la certification est octroyée par l'ANSSI pour une durée maximale de deux ans. Le recours à un service de vérification d'identité à distance certifié au titre du [DECRET_2020-118] permet d'apporter une présomption de conformité aux exigences relatives à la vérification d'identité à distance pour un niveau de garantie donné.

Un même service de vérification d'identité à distance peut être utilisé dans différents cadres réglementaires.

IV. Exigences à respecter par le prestataire

IV.1. Exigences générales

a) Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale.

b) Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de sa prestation et en particulier les éventuels dommages causés à ce commanditaire. À ce titre, le prestataire doit préciser les types de dommages concernés et les modalités de partage des responsabilités dans la convention de service, en tenant compte de toutes les éventuelles activités sous-traitées.

c) Le prestataire doit souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de sa prestation.

d) Le prestataire doit élaborer et tenir à jour un plan d'arrêt d'activité permettant de garantir que les informations pertinentes restent accessibles, pendant une durée appropriée, aux fins de fourniture de preuves en justice et de continuité du service métier.

e) Le prestataire doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.

f) Le prestataire doit apporter une preuve suffisante attestant que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts.

g) Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect des utilisateurs, du commanditaire, de son personnel et de son infrastructure.

h) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

i) Le prestataire doit demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auquel il est soumis et notamment celles relatives à son secteur d'activité.

j) Le prestataire doit établir une convention de service avec le commanditaire répondant aux exigences du chapitre IV.7.2 du présent référentiel et approuvée formellement, par écrit, par le commanditaire avant l'exécution de la prestation.

IV.2. Appréciation et traitement des risques

IV.2.1. Dispositions communes aux appréciations des risques

a) Le prestataire doit élaborer, conformément à la démarche [ISO27005] :

- une appréciation des risques relatifs à l'usurpation d'identité[4] ;
- une appréciation des risques relatifs la sécurité des systèmes d'information[5].

Il est recommandé utilise la méthode [EBIOS_RM] pour élaborer les appréciations des risques.

b) Le prestataire doit réviser les appréciations des risques identifiées à l'exigence IV.2.1.a) au moins annuellement, ainsi que selon les conditions précisées dans les chapitres IV.2.2. et IV.2.3.

c) Le prestataire doit, dans les appréciations des risques identifiées à l'exigence IV.2.1.a), considérer les profils d'attaquants suivants : toute personne, tout groupe de personnes ou toute organisation malveillante, internes ou externes.

[4] Les exigences spécifiques relatives à cette appréciation des risques sont définies au chapitre IV.2.2.

[5] Les exigences spécifiques relatives à cette appréciation des risques sont définies au chapitre IV.2.3.

d) **[SUBSTANTIEL]** Pour le niveau de garantie substantiel, le prestataire doit, dans les appréciations des risques identifiées à l'exigence IV.2.1.a), considérer les attaquants disposant d'un potentiel d'attaque modéré.

e) **[ELEVE]** Pour le niveau de garantie élevé le prestataire doit, dans les appréciations des risques identifiées à l'exigence IV.2.1.a), considérer les attaquants disposant d'un potentiel d'attaque élevé.

f) Le prestataire doit identifier dans les appréciations des risques identifiées à l'exigence IV.2.1.a) l'ensemble des risques résiduels.

g) Le prestataire doit faire valider, formellement et par écrit, par sa direction les appréciations des risques identifiées à l'exigence IV.2.1.a) ainsi que l'ensemble des risques résiduels associés à chacune des appréciations des risques.

h) Le prestataire doit garantir la confidentialité des appréciations des risques identifiées à l'exigence IV.2.1.a).

IV.2.2. Appréciation des risques relatifs à l'usurpation d'identité

a) Le prestataire doit dans cette appréciation des risques, identifier au minimum explicitement l'événement redouté suivant : usurpation d'identité.

b) Le prestataire doit, dans la définition du périmètre de l'appréciation des risques, identifier explicitement les grandes fonctions décrites au chapitre II.1, à savoir :

- 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.

c) Il est recommandé que le prestataire s'inspire de la norme [ISO30107-3] pour identifier les scénarios de risque relatifs à des attaques de présentation en biométrie.

d) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à la contrefaçon et à la falsification de titres d'identité par des moyens physiques, dont au moins les suivants :

- utilisation d'un titre d'identité contrefait pour créer une fausse identité ;
- utilisation d'un titre d'identité contrefait pour usurper l'identité d'une personne existante ;
- utilisation d'un titre d'identité falsifié pour créer une fausse identité ;
- utilisation d'un titre d'identité falsifié pour usurper l'identité d'une personne existante ;

e) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à la contrefaçon et à la falsification de titres d'identité par des moyens numériques, dont au moins les suivants :

- [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] présentation d'un titre « virtuel » (exemple : modélisation d'une image venant se transposer sur la vidéo du titre d'identité) pour créer une fausse identité ;
- [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] injection de données frauduleuses (photographie, données d'identité, etc.) en remplacement des données présentes sur le titre d'identité pour créer une fausse identité ;
- [lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] compromission des secrets cryptographiques ou exploitation d'une vulnérabilité du protocole cryptographique pour modifier les données d'identification extraites du titre d'identité.

f) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à l'altération de l'apparence de l'utilisateur par des moyens physiques, dont au moins les suivants :

- utilisation d'un masque « physique » (exemple : latex) ressemblant à une personne existante pour usurper son identité ;
- utilisation de maquillage pour se grimer et ainsi ressembler à une personne existante pour usurper son identité ;

g) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à l'altération de l'apparence de l'utilisateur par des moyens numériques, dont au moins les suivants :

- utilisation d'un masque « virtuel » (exemple : modélisation d'un masque virtuel à partir de vidéos ou de photographies) ressemblant à une personne existante pour usurper son identité ;
- injection de photographies ou vidéos frauduleuses du visage d'une personne existante en remplacement des données capturées lors de la phase d'acquisition pour usurper son identité.

h) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à la ressemblance de l'utilisateur avec une personne existante pour usurper son identité (sosie, jumeau, etc.).

i) Le prestataire doit dans l'appréciation des risques, identifier les scénarios de risque relatifs à l'influence sur le comportement de l'utilisateur, dont au moins les suivants :

- génération d'une contrainte sur l'utilisateur le forçant à s'identifier à distance (ex. menace physique, chantage, etc.) ;
- piégeage de l'utilisateur en l'invitant à s'identifier à distance auprès d'un service autre que celui auquel il pense accéder, afin de collecter ses données d'identification.

j) Le prestataire doit réviser l'appréciation des risques à chaque modification de la politique de vérification d'identité à distance ou de la déclaration des pratiques de vérification, et en fonction de l'évolution de l'état de l'art et de l'état de la menace.

IV.2.3. Appréciation des risques relatifs à la sécurité des systèmes d'information

a) Le prestataire doit dans cette appréciation des risques identifier explicitement au minimum les événements redoutés suivants :

- fuite de données à caractère personnel ;
- fuite d'informations sensibles relatives aux processus de détection de fraude.

Il est recommandé que le prestataire identifie dans son appréciation des risques des événements redoutés relatifs à la dégradation de l'expérience utilisateur et à l'indisponibilité du système.

b) Le prestataire doit réviser l'appréciation des risques en cas de modification structurante du système d'information du service de vérification d'identité à distance, notamment celles concernant son hébergement, son infrastructure ou son architecture ou de modification de la politique de vérification d'identité.

IV.2.4. Plan de traitement des risques

a) Le prestataire doit élaborer un plan de traitement des risques portant sur l'intégralité du périmètre du service de vérification d'identité électronique et associé à l'ensemble des appréciations des risques identifiées à l'exigence IV.2.1.a).

b) **[SUBSTANTIEL]** Pour le niveau de garantie substantiel, l'application du plan de traitement des risques doit permettre de garantir que le service résiste à des attaquants disposant d'un potentiel d'attaque modéré.

c) **[ELEVE]** Pour le niveau de garantie élevé, l'application du plan de traitement des risques doit permettre de garantir que le service résiste à des attaquants disposant d'un potentiel d'attaque élevé.

d) Le prestataire doit faire valider, formellement et par écrit, par sa direction le plan de traitement des risques.

e) Le prestataire doit établir un suivi périodique de la mise en œuvre du plan de traitement des risques et alerter sa direction en cas d'écart significatif.

f) Le prestataire doit réviser le plan de traitement des risques au minimum annuellement, et en cas de modification de l'une des appréciations des risques identifiées à l'exigence IV.2.1.a).

g) Le prestataire doit assurer la confidentialité du plan de traitement des risques.

IV.2.5. Plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité

a) Le prestataire doit élaborer et tenir à jour un plan destiné à tester la capacité effective du service à détecter des tentatives d'usurpation d'identité

- Pour l'authenticité du titre d'identité :
    - [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] tester l'efficacité des mesures appliquées au titre du plan de traitement des risques pour réduire les risques relatifs à la contrefaçon et à la falsification de titres d'identité par des moyens physiques ou numériques identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité ;
    - [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] mesurer les taux de faux négatifs (FRR) et de faux positifs (FAR) effectivement atteints par le service dans la cadre de la détection des risques relatifs de la contrefaçon et à la falsification de titres d'identité par des moyens physiques ou numériques identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité.
- Pour la détection du vivant :
    - tester l'efficacité des mesures appliquées au titre du plan de traitement des risques pour réduire les risques relatifs à l'altération de l'apparence de l'utilisateur par des moyens physiques ou numériques identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité ;
    - mesurer les taux de faux négatifs (FRR) et de faux positifs (FAR) effectivement atteints par le service dans le cadre de la détection des risques relatifs à l'altération de l'apparence de l'utilisateur par des moyens physiques ou numériques identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité.
- Pour la comparaison du visage de l'utilisateur :
    - tester l'efficacité des mesures appliquées au titre du plan de traitement des risques pour réduire les risques relatifs à la ressemblance native de l'utilisateur avec une autre personne (sosie, jumeau, etc.) ;
    - mesurer les taux de faux négatifs (FRR) et de faux positifs (FAR) effectivement atteints par le service dans le cadre de la comparaison du visage de l'utilisateur et de la photographie figurant dans le titre d'identité.
- Pour les risques relatifs à l'influence sur le comportement de l'utilisateur :
    - tester l'efficacité des mesures appliquées au titre du plan de traitement des risques pour réduire les risques relatifs à l'influence sur le comportement de l'utilisateur identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité.

b) Le plan de test doit être validé par les référents fraude Titre d'identité et Biométrie pour chacun en ce qui le concerne.

c) Le prestataire doit exécuter le plan de test annuellement et à chaque modification structurante du service, mise à jour des appréciations des risques ou du plan de traitement des risques.

d) Le prestataire doit consigner dans un rapport les résultats de chaque exécution du plan de test et faire faire valider ce rapport par les référents fraude Titre d'identité et Biométrie pour chacun en ce qui le concerne.

e) Il est recommandé que les tests relatifs à l'altération de l'apparence de l'utilisateur soient élaborés conformément à la norme [ISO30107-3].

f) Le prestataire doit, si les taux mesurés lors de l'exécution du plan de test sont moins bons que les taux définis dans la politique de vérification d'identité à distance, informer sans délais les référents fraude Titre d'identité et Biométrie pour chacun en ce qui le concerne.

g) Le prestataire doit, si les taux mesurés lors de l'exécution du plan de test sont moins bons que les taux définis dans la politique de vérification d'identité à distance, considérer cette situation comme un incident et, à ce titre, conformément à [PROCESS_CERTIF_SERVICE] et [PROCESS_QUALIF_SERVICE], en informer sans délai l'ANSSI.

h) Le prestataire doit assurer la confidentialité du plan de test et des résultats associés.

IV.3. Politique et pratiques de vérification d'identité à distance

a) Le prestataire doit élaborer et tenir à jour une politique de vérification d'identité à distance[6].

b) La politique de vérification d'identité à distance doit être identifiée de manière unique par un OID, et chacune de ses mises à jour majeures doit faire l'objet d'un OID distinct.

c) Le prestataire doit garantir aux utilisateurs et commanditaires un accès facile, direct et permanent à la politique de vérification d'identité à distance.

d) Le prestataire doit élaborer et tenir à jour une déclaration des pratiques de vérification d'identité à distance, faisant référence à l'OID de la politique de vérification d'identité à distance à laquelle elle se rapporte[7].

e) La déclaration des pratiques de vérification d'identité à distance est confidentielle et ne doit être mise à disposition que des seules personnes ayant le besoin d'en connaître.

IV.3.1. Généralités

a) La politique de vérification d'identité à distance doit identifier les attributs du titre d'identité qui caractérisent l'unicité de l'identité d'une personne physique.

b) La politique de vérification d'identité à distance doit identifier si le service de vérification d'identité à distance est de type « asynchrone », « synchrone avec interaction » ou « synchrone sans interaction ».

c) La déclaration des pratiques de vérification d'identité à distance doit identifier l'ensemble des motifs d'échec de la vérification d'identité à distance qui peuvent être communiqués à l'utilisateur et au service métier. Ces motifs ne doivent pas comporter d'information sur les vérifications réalisées et sur le type de fraude suspecté le cas échéant.

d) La politique de vérification d'identité à distance doit préciser si des données complémentaires sont requises par le service métier et, le cas échéant, les préciser.

e) La politique de vérification d'identité à distance doit indiquer que les données complémentaires

[6] Les informations à faire figurer dans la politique de vérification d'identité à distance sont identifiées dans les chapitres IV.3.1 à IV.3.5.

[7] Les informations à faire figurer dans la déclaration des pratiques de vérification d'identité à distance sont identifiées dans les chapitres IV.3.1 à IV.3.5.

n’entrent pas dans le calcul du verdict de la vérification d’identité à distance.

IV.3.1.1. Fraude

a) La politique de vérification d’identité à distance doit définir les indicateurs permettant de détecter les tentatives d’usurpation d’identité relatives aux scénarios de risque identifiés dans l’appréciation des risques relatifs à l’usurpation d’identité.

b) La déclaration des pratiques de vérification d’identité à distance doit décrire les moyens techniques et organisationnels mis en œuvre par le prestataire pour mesurer les indicateurs permettant de détecter les tentatives d’usurpation d’identité (exigence IV.3.1.1.a).

c) La politique de vérification d’identité à distance doit indiquer qu’à chaque usurpation d’identité suspectée ou avérée, qu’elle soit détectée par le prestataire (exigence IV.3.1.1.b) ou communiquée par le service métier, une alerte est générée.

d) La déclaration des pratiques de vérification d’identité à distance doit identifier les procédures de traitement des alertes générées lorsque qu’une usurpation d’identité est suspectée ou avérée (exigence IV.3.1.1.c). Ces procédures doivent prévoir l’information systématique du référent fraude Titre d’identité lorsque l’usurpation d’identité suspectée ou avérée concerne le titre d’identité, et l’information systématique du référent fraude Biométrie lorsque l’usurpation d’identité suspectée ou avérée concerne la biométrie.

e) La déclaration des pratiques de vérification d’identité à distance doit préciser les mesures mises en œuvre par le prestataire pour notifier à l’utilisateur la nature de l’opération en cours, et prévenir les risques de piégeage de l’utilisateur.

f) La politique de vérification d’identité à distance doit préciser les voies de recours offertes aux utilisateurs du service, notamment à des fins d’annulation d’une identification frauduleuse ou en cas de refus d’identification d’un utilisateur de bonne foi.

IV.3.1.2. Données à caractère personnel

a) La politique de vérification d’identité à distance doit décrire les alternatives à la vérification d’identité à distance offertes aux utilisateurs le cas échéant.

b) La politique de vérification d’identité à distance doit préciser que le prestataire respecte le principe de minimisation des données collectées et conservées.

c) La politique de vérification d’identité à distance doit identifier l’ensemble des données à caractère personnel relatives aux utilisateurs traitées par le service de vérification d’identité à distance.

d) La politique de vérification d’identité à distance doit identifier parmi l’ensemble des données à caractère personnel relatives aux utilisateurs traitées par le service, lesquelles peuvent faire l’objet d’un traitement biométrique.

e) La politique de vérification d’identité à distance doit identifier, pour chaque donnée à caractère personnel relative aux utilisateurs traitée par le service de vérification d’identité à distance : la durée de conservation selon le verdict « succès » ou « échec », les modalités de conservation, de destruction, d’accès et de rectification offertes aux utilisateurs, ainsi que les traitements réalisés par le prestataire sur ces données. La durée de conservation doit être proportionnée à la finalité. Au regard du principe de responsabilisation, il importe au responsable de traitement de définir une durée de conservation.

f) La politique de vérification d’identité doit préciser que la durée de conservation des données dont la finalité est de faire l’objet d’un traitement biométrique ne doit pas excéder quatre-vingt-seize heures.

g) La politique de vérification d’identité à distance doit préciser la ou les finalités de conservation des données à caractère personnel relatives aux utilisateurs traitées par le service de vérification.

h) Il est recommandé que le responsable de traitement s’appuie sur le guide [CNIL_Guide_conservation] pour définir les durées et modalités de conservation.

i) La politique de vérification d'identité à distance doit interdire la rectification ou la suppression par l'utilisateur du dossier de preuve et des résultats de la vérification d'identité à distance transmis au service métier, ainsi que de l'ensemble des informations nécessaires à la constitution du résultat.

j) La politique de vérification d'identité à distance doit interdire l'accès de l'utilisateur aux données ayant fait l'objet de traitements automatisés ou manuels dont la communication est susceptible de renseigner sur la nature des vérifications réalisées par le service et relatives à la détection d'usurpation d'identité.

IV.3.1.3. Langages

a) La politique de vérification d'identité à distance doit identifier l'ensemble des langues supportées par le service de vérification d'identité à distance.

b) La politique de vérification d'identité à distance doit indiquer que le service supporte au moins la langue française.

c) La politique de vérification d'identité à distance doit indiquer que le service, préalablement à l'acquisition des données d'identification, demande à l'utilisateur la langue qu'il souhaite utiliser, lorsque le service supporte une ou plusieurs langues autres que la langue française.

d) La politique de vérification d'identité à distance doit indiquer que le service informe l'utilisateur du pays dans lequel se trouve les opérateurs chargés de réaliser les vérifications et de prononcer le verdict de la vérification d'identité à distance.

IV.3.1.4. Enregistrement et traitement des réclamations

a) La politique de vérification d'identité à distance doit indiquer que le prestataire met à disposition du commanditaire, des utilisateurs et des tiers un processus d'enregistrement et de traitement des réclamations relatives au service de vérification d'identité à distance.

b) La politique de vérification d'identité à distance doit décrire le processus d'enregistrement et de traitement des réclamations.

IV.3.2. Acquisition

IV.3.2.1. Terminal

a) La politique de vérification d'identité à distance doit identifier si l'acquisition des données d'identification relatives aux utilisateurs est réalisée par le terminal de l'utilisateur ou un terminal du prestataire ou du service métier.

b) La politique de vérification d'identité à distance doit, lorsque l'acquisition des données d'identification relatives aux utilisateurs est réalisée par le terminal de l'utilisateur, préciser si l'installation d'une application sur le terminal de l'utilisateur est requise.

IV.3.2.2. Titres d'identité

a) La politique de vérification d'identité à distance doit indiquer qu'elle ne peut être mise à jour concernant les sujets relatifs aux titres d'identité qu'après validation formelle du référent fraude Titre d'identité.

b) La politique de vérification d'identité à distance doit identifier les demandes qui peuvent être formulées par le service à l'utilisateur pour une acquisition correcte du titre d'identité (luminosité, mise au point, reflets, etc.).

c) La déclaration des pratiques de vérification d'identité à distance doit décrire les mécanismes mis en œuvre pour que l'acquisition de la vidéo du titre d'identité ne soit pas prédictible, et par conséquent non réutilisable par un attaquant.

IV.3.2.3. Visage

a) La politique de vérification d'identité à distance doit indiquer qu'elle ne peut être mise à jour concernant les sujets relatifs à la biométrie qu'après validation formelle du référent fraude Biométrie.

b) La politique de vérification d'identité à distance doit décrire les demandes qui peuvent être formulées par le service à l'utilisateur dans le cadre des étapes d'acquisition et de vérification des données d'identification (ex. : luminosité, mise au point, retrait des lunettes de l'utilisateur, etc.).

c) La déclaration des pratiques de vérification d'identité à distance doit décrire les mécanismes mis en œuvre pour que l'acquisition de la vidéo du visage ne soit pas prédictible et par conséquent non réutilisable par un attaquant.

IV.3.3. Vérification

IV.3.3.1. Terminal

a) La politique de vérification d'identité à distance doit préciser que, lorsque le terminal est celui de l'utilisateur, aucun contrôle réalisé sur le terminal de l'utilisateur ne peut contribuer au verdict « succès » de la vérification d'identité à distance.

b) La politique de vérification d'identité à distance doit, lorsque le terminal est celui du prestataire ou du service métier, préciser si des traitements, même partiels, relatifs à la vérification de l'authenticité du titre d'identité, à la correspondance du visage de l'utilisateur avec la photographie extraite du titre d'identité ou à la vérification de la preuve du vivant sont réalisés sur le terminal. Le cas échéant, la déclaration des pratiques de vérification d'identité à distance doit préciser ces traitements.

IV.3.3.2. Titres d'identité

a) La politique de vérification d'identité à distance doit identifier les titres d'identité acceptés par le service de vérification d'identité à distance. Ces titres d'identité doivent figurer dans la liste fournie en Annexe 4.

b) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit identifier, pour chaque titre d'identité accepté, les éléments de sécurité vérifiés par le service. Le prestataire peut notamment s'appuyer sur le registre public en ligne des documents authentiques d'identité et de voyage (PRADO[8]) pour l'identification des éléments de sécurité associés à chaque titre d'identité.

c) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit, pour chaque élément de sécurité vérifié des titres d'identités acceptés, décrire l'ensemble des vérifications réalisées, préciser pour chaque vérification si elle est réalisée de manière automatisée ou par un opérateur humain, et si elle est réalisée de manière systématique ou uniquement sous certaines conditions. Le cas échéant, ces conditions sont décrites.

d) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit identifier, pour chaque titre d'identité accepté, les éléments de sécurité du titre d'identité non vérifiés par le prestataire et figurant dans le registre public en ligne des documents authentiques d'identité et de voyage (PRADO[8]) et, pour chaque élément de sécurité non vérifié par le service, fournir une justification.

e) La politique de vérification d'identité à distance doit indiquer que le prestataire élabore et tient à jour une liste identifiant pour chaque titre d'identité accepté au moins un référent fraude Titre d'identité compétent.

[8] Voir acronyme au chapitre I.3.1.

f) La politique de vérification d'identité à distance doit indiquer que seuls les titres non-expirés sont acceptés par le service.

g) La déclaration des pratiques de vérification d'identité à distance doit identifier, pour chaque titre d'identité accepté, si une vérification de validité[9] du titre d'identité via un service mis à disposition par l'État émetteur est réalisée, et le cas échéant :

- identifier le service de vérification de validité ;
- préciser si cette vérification de validité est réalisée de manière automatisée ou par un opérateur humain ;
- préciser si cette vérification de validité est réalisée de manière systématique ou uniquement sous certaines conditions, et le cas échéant, décrire ces conditions ;
- préciser les conséquences si le service de vérification de validité est indisponible.

h) La politique de vérification d'identité à distance doit indiquer que le prestataire vérifie systématiquement que le titre d'identité est valide dès lors qu'un tel service est mis à disposition du prestataire par l'État responsable de l'émission du titre d'identité.

i) La politique de vérification d'identité à distance doit indiquer que, si une vérification de validité du titre d'identité est réalisée et que cette dernière conclut que le titre d'identité est invalide, alors le verdict de la vérification d'identité à distance est systématiquement « échec ».

j) La déclaration des pratiques de vérification d'identité à distance doit préciser si des mesures de sécurité particulières sont appliquées pour certains types d'utilisateurs afin de renforcer les contrôles destinés à empêcher une usurpation d'identité, et le cas échéant, préciser ces mesures.

k) La déclaration des pratiques de vérification d'identité à distance doit préciser les mesures mises en œuvre le cas échéant pour limiter les tentatives d'attaques récurrentes.

l) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la politique de vérification d'identité à distance doit décrire comment sont vérifiés les titres d'identité présentant une altération physique (titre d'identité déchiré ou écorné, etc.).

m) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la politique de vérification d'identité à distance doit indiquer que la résolution minimale après compression de la vidéo du titre d'identité acceptée par le service. Cette résolution minimale ne peut être inférieure à 720p : 1280 × 720 à 25 images par seconde.

n) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit décrire les contrôles[10] réalisés par le service de vérification d'identité à distance sur la qualité de la vidéo du titre d'identité acquise. Ces contrôles comprennent au minimum la résolution identifiée à l'exigence IV.3.3.2.m) et peuvent être complétés par d'autres contrôles : luminosité de l'environnement, etc.

o) [Lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] la politique de vérification d'identité à distance doit indiquer que le verdict rendu par le service est automatiquement « échec », sans intervention d'un opérateur, si les traitements automatisés relatifs à la vérification de l'authenticité du titre d'identité concluent que le titre n'est pas authentique.

p) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit indiquer

[9] La confirmation de validité suppose au moins que le titre est connu comme existant, n'est pas expiré, et n'a pas été déclaré perdu ou volé ou fait l'objet d'une invalidation pour tout autre motif. Selon le service considéré, celui-ci peut indiquer uniquement si le titre concerné est valide ou invalide, ou indiquer des motifs d'invalidité (déclaré perdu, déclaré volé). L'information relative à la validité est suffisante pour répondre aux exigences du référentiel.

[10] Ces contrôles sont à dissocier des éventuels contrôles réalisés sur le terminal.

les taux de faux négatifs (FRR) et de faux positifs (FAR) acceptés par le service pour la vérification de l'authenticité du titre d'identité.

q) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur prononce un verdict « succès » alors que les résultats des traitements automatisés relatifs à l'authenticité du document d'identité proposent un verdict « échec ». Ces procédures doivent prévoir au minimum une alerte auprès du référent fraude Titre d'identité.

r) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur prononce un verdict « échec » alors que les résultats des traitements automatisés relatifs à l'authenticité du document d'identité proposent un verdict « succès ». Ces procédures doivent prévoir au moins un enregistrement de l'événement à des fins d'analyse.

s) **[ELEVE]** La politique de vérification d'identité à distance doit indiquer que l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité du titre d'identité. En cas d'impossibilité technique ou juridique d'exploiter le composant de sécurité du titre d'identité, ou si le titre d'identité est dépourvu de composant de sécurité, le titre d'identité ne peut être accepté.

t) **[ELEVE]** La politique de vérification d'identité à distance doit indiquer que, pour chaque titre d'identité accepté, la validité du titre d'identité est systématiquement vérifiée en s'appuyant sur un service mis à disposition par l'État émetteur du titre d'identité. À défaut d'existence ou d'accès à ce service, ou en cas d'indisponibilité, le titre d'identité ne peut être accepté.

IV.3.3.3. Comparaison du visage

a) La politique de vérification d'identité à distance doit indiquer la résolution minimale après compression de la vidéo du visage de l'utilisateur acceptée par le service. Cette résolution ne peut être inférieure à 720p : 1280 × 720 à 25 images par seconde.

b) La déclaration des pratiques de vérification d'identité à distance doit décrire les contrôles réalisés[11] par le service de vérification d'identité à distance sur la qualité de la vidéo du visage de l'utilisateur acquise. Ces contrôles comprennent au minimum la résolution identifiée à l'exigence IV.3.3.3.a) et peuvent être complétés par d'autres contrôles : luminosité de l'environnement, etc.

c) La déclaration des pratiques de vérification d'identité à distance doit décrire l'ensemble des vérifications réalisées dans le cadre de la comparaison entre le visage de l'utilisateur et la photographie du titre d'identité, et préciser pour chaque vérification si elle est réalisée de manière automatisée ou par un opérateur humain, et si elle est réalisée de manière systématique ou uniquement sous certaines conditions. Le cas échéant, ces conditions sont décrites dans la déclaration des pratiques de vérification d'identité à distance.

d) La déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur prononce un verdict « succès » alors que les résultats des traitements automatisés relatifs à la comparaison du visage de l'utilisateur proposent un verdict « échec ». Ces procédures doivent prévoir au minimum une alerte auprès du référent fraude Biométrie.

e) La déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur prononce un verdict « échec » alors que les résultats des traitements automatisés relatifs à la comparaison du visage de l'utilisateur proposent un verdict « succès ». Ces procédures doivent prévoir au moins un enregistrement de l'événement à des fins d'analyse.

f) La déclaration des pratiques de vérification d'identité à distance doit indiquer les taux de faux négatifs (FRR) et de faux positifs (FAR) acceptés par le service pour la comparaison du visage de l'utilisateur.

[11] Ces contrôles sont à dissocier des éventuels contrôles réalisés sur le terminal.

g) [Lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] la politique de vérification d'identité à distance doit indiquer que la photographie utilisée pour réaliser la comparaison du visage est celle extraite du composant de sécurité.

IV.3.3.4. Détection du vivant

a) La déclaration des pratiques de vérification d'identité à distance doit décrire l'ensemble des vérifications réalisées dans le cadre de la détection du vivant et préciser pour chaque vérification si elle est réalisée de manière automatisée ou par un opérateur humain. Le cas échéant, ces conditions sont décrites.

b) La déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur propose un verdict « succès » alors que les résultats des traitements automatisés relatifs à la détection du vivant proposent un verdict « échec ». Ces procédures doivent prévoir au minimum une alerte auprès du référent fraude Biométrie.

c) La déclaration des pratiques de vérification d'identité à distance doit préciser les procédures appliquées lorsqu'un opérateur prononce un verdict « échec » alors que les résultats des traitements automatisés relatifs à la détection du vivant proposent un verdict « succès ». Ces procédures doivent prévoir au moins un enregistrement de l'événement à des fins d'analyse.

d) La déclaration des pratiques de vérification d'identité à distance doit indiquer les taux de faux négatifs (FRR) et de faux positifs (FAR) acceptés par le service pour la détection du vivant.

IV.3.4. Constitution du dossier de preuve

a) La politique de vérification d'identité à distance doit indiquer que chaque vérification d'identité quel que soit le verdict (« succès » ou « échec ») fait l'objet de la création d'un dossier de preuve.

b) La politique de vérification d'identité à distance doit identifier les éléments constitutifs du dossier de preuve. Ces éléments doivent permettre de fournir toutes les informations nécessaires à la résolution des litiges.

c) La politique de vérification d'identité à distance doit indiquer que le dossier de preuve contient au moins les éléments suivants :
- les données d'identification :
    - [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la vidéo du titre d'identité
    - [lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] la photographie de l'utilisateur extraite du composant de sécurité du titre d'identité
    - la vidéo du visage de l'utilisateur
- la date d'acquisition de chaque donnée d'identification
- la liste de l'ensemble des vérifications réalisées sur les données d'identification, et pour chaque vérification :
    - la date de la vérification
    - l'activité associée à la vérification, notamment :
        - vérification de l'authenticité du titre d'identité
        - détection du caractère « vivant » de l'utilisateur
        - comparaison du visage de l'utilisateur
    - la nature de la vérification : automatique ou manuelle
    - l'identité de l'opérateur ou du référent fraude qui a procédé à la vérification lorsque cette dernière est manuelle
    - le pays depuis lequel l'opérateur ou le référent fraude a réalisé la vérification lorsque cette dernière est manuelle
    - la version et la configuration le cas échéant des outils ayant réalisé la vérification cette dernière est automatique

    - le constat intermédiaire rendu par les traitements automatisés, l'opérateur ou le référent fraude suite à la vérification
- le verdict de la vérification d'identité à distance (succès ou échec)
- les motifs rendus par l'opérateur en cas de verdict « échec »
- l'identité de l'opérateur qui a prononcé le verdict
- la date à laquelle le verdict a été prononcé par l'opérateur
- le pays depuis lequel l'opérateur a prononcé le verdict
- les noms et prénoms de l'utilisateur
- la date et le lieu de naissance de naissance de l'utilisateur
- le numéro unique du titre d'identité
- la date de délivrance du titre d'identité
- la date d'expiration du titre d'identité
- le résultat de la vérification d'identité à distance transmis au service métier.

d) La politique de vérification d'identité à distance doit indiquer que le dossier de preuve ne contient aucune donnée ayant pour finalité un traitement biométrique.

e) La durée de conservation des dossiers de preuve doit tenir compte de la durée pendant laquelle peut survenir un contentieux.

f) La politique de vérification d'identité à distance doit indiquer que le prestataire chiffre les dossiers de preuve dès leur création, et précise si la clé de déchiffrement est mise en œuvre dans un équipement cryptographique sécurisé.

g) La politique de vérification d'identité à distance doit préciser que les dossiers de preuve chiffrés sont conservés hors-ligne si la clé de déchiffrement n'est pas mise en œuvre dans un équipement cryptographique sécurisé.

h) La politique de vérification d'identité à distance doit préciser les modalités de gestion de la clé de déchiffrement du dossier de preuve et notamment limiter l'accès à cette clé aux seules personnes ayant le besoin d'en connaitre.

i) La politique de vérification d'identité à distance doit indiquer que les utilisateurs peuvent exercer leur droit d'accès aux données à caractère personnel les concernant détenues par le prestataire dans le dossier de preuve, mais ne peuvent exercer de droit de rectification sur ce dossier.

j) La déclaration des pratiques de vérification d'identité à distance doit indiquer si la vidéo du visage de l'utilisateur est compressée avec perte lorsqu'elle conservée dans le dossier de preuve. Le cas échéant, les informations relatives à la méthode de compression avec perte sont décrites.

k) [Lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] la déclaration des pratiques de vérification d'identité à distance doit indiquer si la vidéo du titre d'identité est compressée avec perte lorsqu'elle conservée dans le dossier de preuve. Le cas échéant, les informations relatives à la méthode de compression avec perte sont décrites.

IV.3.5. Transmission du résultat

a) La politique de vérification d'identité à distance doit indiquer que le résultat de la vérification d'identité à distance est transmis au service métier systématiquement, quel que soit le verdict (succès ou échec).

b) La politique de vérification d'identité à distance doit indiquer que le résultat de la vérification d'identité à distance n'est constitué que du verdict (succès ou échec) de la vérification et des attributs d'identité relatifs à l'utilisateur (ex. : nom(s), prénom(s), sexe, date de naissance, lieu de naissance, numéro du titre d'identité, une photographie du visage de l'utilisateur extraite de la vidéo du visage de l'utilisateur, une photographie du titre d'identité extraite de la vidéo du titre d'identité de l'utilisateur etc.), ainsi que des éventuelles données complémentaires demandées par le service métier.

c) La politique de vérification d'identité à distance doit identifier les attributs d'identité relatifs aux utilisateurs contenus dans le résultat de la vérification d'identité.

d) La politique de vérification d'identité à distance doit indiquer que les vidéos du titre d'identité et du visage de l'utilisateur ne sont d'aucune manière, totalement ou partiellement[12], transmises au service métier.

e) La politique de vérification d'identité à distance doit indiquer le délai maximal entre le début de l'acquisition des données d'identification de l'utilisateur et la notification du résultat de la vérification d'identité au service métier. Ce délai ne peut excéder quatre-vingt-seize heures.

f) La politique de vérification d'identité à distance doit indiquer que le résultat de la vérification d'identité à distance ne contient aucun élément relatif aux constats issus des vérifications réalisées par le service autre que le verdict indiqué à l'exigence IV.3.5.b), et notamment aucun score calculé sur la base de ces vérifications.

IV.4. Activités du service de vérification d'identité à distance

IV.4.1. Acquisition des données d'identification

IV.4.1.1. Acquisition du titre d'identité

a) Le prestataire doit acquérir une vidéo du titre d'identité conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

IV.4.1.2. Acquisition du visage

a) Le prestataire doit acquérir une vidéo du visage de l'utilisateur conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

IV.4.2. Vérification des données d'identification

IV.4.2.1. Vérification de l'authenticité du titre d'identité

a) Le prestataire doit vérifier l'authenticité du titre conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

IV.4.2.2. Vérification de la correspondance du visage

a) Le prestataire doit vérifier la correspondance du visage de l'utilisateur avec la photographie extraite du titre d'identité conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

IV.4.2.3. Détection du vivant

a) Le prestataire doit détecter le caractère « vivant » de l'utilisateur conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

IV.4.3. Constitution du dossier de preuve

a) Le prestataire doit générer une preuve conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

[12] Une photographie du visage de l'utilisateur extraite de la vidéo du visage de l'utilisateur et une photographie du titre d'identité extraite de la vidéo du titre d'identité peuvent néanmoins faire partie du résultat de la vérification d'identité à distance, conformément à l'exigence IV.3.5.b)

IV.4.4. Transmission des résultats

a) Le prestataire doit, pour chaque identité vérifiée, générer un résultat conformément à la politique de vérification d'identité à distance et à la déclaration des pratiques de vérification d'identité à distance.

b) Le prestataire doit transmettre le résultat au service métier conformément à la politique de sécurité des systèmes d'information.

IV.5. Protection de l'information

IV.5.1. Terminal

a) Le prestataire doit protéger en confidentialité et en intégrité les données d'identification échangées entre le terminal, qu'il s'agisse du terminal de l'utilisateur, du terminal du prestataire ou du terminal du service métier, et le service de vérification d'identité à distance.

b) Le prestataire doit authentifier le terminal lorsque ce dernier est sous sa responsabilité ou celle du service métier (authentification par certificat par exemple).

c) Le prestataire doit, si le service nécessite l'installation d'une application spécifique[13] sur le terminal de l'utilisateur, mettre en œuvre les mesures permettant de s'assurer que cette application ne diminue pas le niveau de sécurité du terminal. La qualification de cette application au niveau élémentaire [PROCESS_QUALIF_PRODUIT] est un moyen d'attester du respect de cette exigence.

Il est recommandé, si le service exige l'installation d'une application spécifique sur le terminal de l'utilisateur, que celle-ci dispose de mécanismes permettant de limiter le risque d'altération ou de substitution de cette application.

d) **[ELEVE]** Le prestataire doit, si le service nécessite l'installation d'une application spécifique sur le terminal de l'utilisateur, faire qualifier cette application au niveau élémentaire [PROCESS_QUALIF_PRODUIT] afin de garantir qu'elle ne diminue pas le niveau de sécurité du terminal.

e) Le prestataire doit, si le service nécessite l'installation d'une application spécifique sur le terminal de l'utilisateur, mettre à disposition des utilisateurs cette application sur les magasins d'applications officiels.

f) Le prestataire doit, si le service nécessite l'installation d'une application spécifique sur le terminal de l'utilisateur et que cette dernière est mise à disposition des utilisateurs sur les magasins d'applications officiels, réaliser une veille pour détecter sur les magasins d'applications officiels la mise à disposition d'applications frauduleuses visant à se substituer à celle, légitime, du service.

IV.5.2. Politique de sécurité des systèmes d'information

a) Le prestataire doit définir et mettre en œuvre une politique de sécurité des systèmes d'information basée sur l'appréciation des risques relatifs à la sécurité des systèmes d'information identifiée au chapitre IV.2.3 et le plan de traitement des risques associé.

b) Le prestataire doit réviser la politique de sécurité des systèmes d'information au minimum tous les deux ans, et en cas de modification de l'appréciation des risques ou du plan de traitement des risques.

c) Le prestataire doit faire valider, formellement et par écrit, par sa direction la politique de sécurité des systèmes d'information.

[13] Est considérée comme « spécifique » une application qui n'est pas liée au service métier mais dont l'installation est requise par le prestataire afin de permettre la vérification d'identité à distance. Une application fournie par le service métier intégrant en complément de ses fonctions natives une interface avec le service du prestataire n'est pas considérée comme une application spécifique.

IV.5.3. Homologation

a) Le prestataire doit homologuer le système d'information du service de vérification d'identité à distance.

> Il est recommandé que le prestataire utilise la démarche décrite dans le guide [HOMOLOGATION] pour homologuer le système d'information du service de vérification d'identité à distance.
>
> Il est recommandé que le prestataire fasse appel à une prestation d'audit de la sécurité des systèmes d'information qualifiée au titre du décret [DECRET_2015-350] dans le cadre de l'homologation.

b) **[ELEVE]** Le prestataire doit respecter les règles relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles [II_901].

c) **[ELEVE]** Le prestataire doit faire appel à une prestation d'audit de la sécurité des systèmes d'information qualifiée au titre de [DECRET_2015-350] dans le cadre de l'homologation. Le plan d'audit élaboré par le PASSI doit comporter au minimum les activités d'audit suivantes: audit organisationnel et physique, audit de configuration, audit d'architecture et tests d'intrusion.

d) Le prestataire doit faire valider, formellement et par écrit, par sa direction la décision d'homologation.

IV.5.4. Territorialité du service

a) Le prestataire doit héberger et traiter les données relatives au service de vérification d'identité à distance exclusivement au sein du territoire d'un État membre de l'Union Européenne.

b) Le prestataire doit exploiter et administrer le service de vérification d'identité à distance exclusivement depuis le territoire d'un État membre de l'Union Européenne.

IV.5.5. Niveau de sécurité

a) [Lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] le prestataire doit protéger en intégrité et, le cas échéant, en confidentialité, l'ensemble des données permettant d'authentifier les calculs cryptographiques réalisés par le composant de sécurité du titre d'identité.

b) Le prestataire doit restreindre les accès des opérateurs au système d'information du service de vérification d'identité à distance au strict nécessaire pour la réalisation de leurs missions.

c) Le prestataire doit respecter les exigences du référentiel [SecNumCloud] si le service est hébergé dans le cadre d'une prestation d'informatique en nuage. La qualification [SecNumCloud] permet de répondre à cette exigence.

d) **[SUBSTANTIEL]** Le prestataire doit appliquer l'ensemble des règles du niveau standard du guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service de vérification d'identité à distance.

> Il est recommandé que le prestataire applique l'ensemble des règles du niveau renforcé du guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service de vérification d'identité à distance. Il est recommandé que le prestataire, pour chaque règle du niveau renforcé, identifie s'il respecte ou non la règle, et que pour chaque règle niveau renforcé qu'il déclare respecter, il décrive les mesures mises en place pour respecter la règle, et que pour chaque règle niveau renforcé qu'il déclare ne pas respecter, il apporte une justification.

e) **[ELEVE]** Le prestataire doit traiter et conserver l'information sensible (susceptible d'influer sur le résultat de la vérification, de porter atteinte à la vie privée des utilisateurs, ou d'affecter la capacité du service à fournir des éléments de preuve en cas de litige) sur un réseau de classe 1 conformément à l'annexe 2 de l'instruction interministérielle relative à la protection des systèmes d'information sensibles [II_901].

f) **[ELEVE]** Le prestataire doit appliquer l'ensemble des règles du niveau renforcé du guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service de vérification d'identité à distance.

g) **[ELEVE]** Le prestataire doit, pour chaque recommandation de [ADMIN_SEC], identifier s'il respecte ou non la recommandation. Pour chaque recommandation qu'il déclare respecter, le prestataire doit décrire les mesures mises en place pour respecter la recommandation. Pour chaque recommandation qu'il déclare ne pas respecter, le prestataire doit apporter une justification.

h) **[ELEVE]** Le prestataire doit, pour chaque recommandation de [ARCHI_DR] relative à la sécurité des informations sensibles, identifier s'il respecte ou non la recommandation. Pour chaque recommandation qu'il déclare respecter, le prestataire doit décrire les mesures mises en place pour respecter la recommandation. Pour chaque recommandation qu'il déclare ne pas respecter, le prestataire doit apporter une justification.

i) **[ELEVE]** Le prestataire doit, pour chaque recommandation de [INTERCO_INTERNET], identifier s'il respecte ou non la recommandation. Pour chaque recommandation qu'il déclare respecter, le prestataire doit décrire les mesures mises en place pour respecter la recommandation. Pour chaque recommandation qu'il déclare ne pas respecter, le prestataire doit apporter une justification.

IV.5.6. Contrôles

a) Le prestataire doit élaborer et mettre en œuvre un plan de contrôle portant sur l'intégralité du périmètre du service de vérification d'identité à distance visant à s'assurer que la politique de sécurité des systèmes d'information, la politique de vérification d'identité à distance, et la déclaration des pratiques de vérification d'identité à distance sont appliquées.

b) Le prestataire doit réviser le plan de contrôle au minimum annuellement et en cas de modification structurante du système d'information du service de vérification d'identité à distance, notamment celles concernant son hébergement, son infrastructure et son architecture, ou en cas de modification structurante de l'appréciation des risques, du plan de traitement des risques, de la politique de sécurité des systèmes d'information, de la politique de vérification d'identité à distance ou de la déclaration des pratiques de vérification d'identité à distance.

c) Le prestataire doit mettre à jour le plan de traitement des risques pour intégrer les résultats des contrôles.

d) Le prestataire doit faire valider par sa direction, formellement et par écrit, les résultats des contrôles.

IV.5.7. Sécurité physique

a) Le prestataire doit élaborer et tenir à jour la liste des personnes autorisées à accéder aux locaux hébergeant le système d'information du service de vérification d'identité à distance.

b) Le prestataire doit mettre en œuvre les mécanismes permettant de garantir que seules les personnes autorisées peuvent accéder aux locaux hébergeant le système d'information du service de vérification d'identité à distance.

c) Le prestataire doit mettre en œuvre les mécanismes permettant de journaliser les accès aux locaux hébergeant le système d'information du service de vérification d'identité à distance.

d) Le prestataire doit définir et mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des journaux d'accès aux locaux hébergeant le service de vérification d'identité à distance.

IV.5.8. Journalisation

a) Le prestataire doit journaliser l'ensemble des traitements automatisés et des actions réalisées par les opérateurs et référents fraude dans le cadre d'une vérification d'identité à distance, et les centraliser sur un composant du système d'information du service auquel les opérateurs et les référents fraude ne disposent d'aucun accès.

b) Le prestataire doit réaliser une corrélation des journaux entre les différents composants du système d'information du service de vérification d'identité à distance.

c) L'ensemble des actions réalisées par les opérateurs et référents fraude doit faire l'objet d'un enregistrement et pouvoir être consulté à des fins d'audit.

d) Le prestataire doit procéder à une revue par échantillonnage des journaux, et notamment des opérations réalisées par les opérateurs et les référents fraude.

IV.5.9. Sauvegardes

a) Le prestataire doit élaborer et mettre en œuvre un plan de sauvegarde et de restauration des dispositifs du service de vérification d'identité à distance, comportant au minimum : sauvegarde des systèmes, des configurations et des données.

Il est recommandé que le prestataire teste le plan de sauvegarde et de restauration au minimum une fois par an.

b) Le prestataire doit définir et mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes, au même niveau que celui pour lequel le service de vérification d'identité à distance a été homologué.

Il est recommandé que le prestataire respecte l'ensemble des mesures et préconisations sur la sécurisation des sauvegardes de [ISO27002].

IV.5.10. Cloisonnement du système d'information du service

a) Le prestataire doit élaborer et maintenir à jour une description détaillée de l'architecture du système d'information du service de vérification d'identité à distance.

Il est recommandé que le système d'information soit dédié exclusivement au service de vérification d'identité à distance et que toute autre prestation soit réalisée sur un système d'information cloisonné physiquement du système d'information du service.

b) Le prestataire doit élaborer et tenir à jour la matrice des flux du service de vérification d'identité à distance, ainsi que la politique de filtrage associée, qui ne doit autoriser que les flux strictement nécessaires au fonctionnement du service de vérification d'identité à distance.

IV.5.11. Administration et exploitation du service

a) Les postes de travail des administrateurs, des opérateurs et des référents fraude doivent être raccordés exclusivement au système d'information du service de vérification d'identité à distance.

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

IV.5.12. Interconnexions du système d'information du service

a) Le prestataire doit identifier dans la description détaillée de l'architecture du système d'information du service de vérification d'identité à distance identifiée à l'exigence IV.5.10.a) l'ensemble des interconnexions du système d'information du service de vérification d'identité avec des systèmes d'information tiers, notamment le système d'information du service métier.

b) Le prestataire doit filtrer tous les flux aux interconnexions du système d'information du service de vérification d'identité à distance.

[SUBSTANTIEL] Il est recommandé que l'ensemble des flux aux interconnexions du système d'information du service de vérification d'identité à distance soit filtré à l'aide de solutions de filtrage qualifiées au niveau standard par l'ANSSI.

c) Le service doit réaliser une authentification mutuelle auprès du service métier lorsqu'il lui transmet les résultats, et garantir l'intégrité, la confidentialité et l'impossibilité de rejouer des données transmises.

d) **[ELEVE]** Le prestataire doit mettre en conformité l'ensemble des interconnexions du système d'information du service de vérification d'identité à distance avec l'Annexe 2 de l'instruction interministérielle relative à la protection des systèmes d'information sensibles [II_901].

IV.5.13. Accès distants

Les exigences du présent chapitre ne sont applicables que si le prestataire permet à tout ou partie de son personnel d'accéder à distance au système d'information du service de vérification d'identité à distance.

a) Le prestataire doit, pour chaque recommandation du guide [NOMADISME], identifier s'il respecte ou non la recommandation. Pour chaque recommandation qu'il déclare respecter, le prestataire doit décrire les mesures mises en place pour respecter la recommandation. Pour chaque recommandation qu'il déclare ne pas respecter, le prestataire doit apporter une justification.

b) Le prestataire doit mettre en place une passerelle dédiée aux accès distants conforme à [NT_ADMIN].

Il est recommandé de mettre en place des passerelles distinctes pour les accès distants des administrateurs et des opérateurs.

c) Le prestataire doit, s'il utilise une passerelle unique pour les accès à distance des administrateurs et des opérateurs, mettre en œuvre une solution permettant d'assurer une séparation stricte des flux des administrateurs et des opérateurs.

d) Les postes nomades utilisés par les administrateurs et les opérateurs doivent être dédiés aux prestations de vérification d'identité à distance.

e) Les administrateurs et opérateurs doivent s'authentifier avec au minimum deux facteurs sur leur poste nomade.

Il est recommandé que le prestataire mette en œuvre pour les accès distants une authentification basée sur des certificats électroniques délivrés par des prestataires de services de certification électronique qualifiés par l'ANSSI selon le RGS [RGS] au niveau deux ou trois étoiles (**/***) et impliquant par conséquent l'utilisation de supports cryptographiques qualifiés par l'ANSSI au niveau standard ou renforcé.

f) Les postes nomades doivent disposer 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.

g) Les postes nomades ne doivent permettre que l'usage de supports amovibles autorisés par la politique de sécurité des systèmes d'information.

h) Les postes nomades doivent avoir l'intégralité de leurs disques chiffrée avec des mécanismes cryptographiques conformes à [CRYPTO_B1].

Il est recommandé que la solution de chiffrement des disques des postes nomades soit qualifiée par l'ANSSI au niveau standard et utilisée conformément aux conditions figurant dans la décision de qualification.

Il est recommandé que les flux entre les postes nomades et les passerelles soient chiffrés à l'aide de solutions de chiffrement et d'authentification *IPsec* qualifiées par l'ANSSI au niveau standard et utilisées conformément aux conditions figurant dans leur décision de qualification.

i) Les postes nomades doivent être configurés pour ne pouvoir communiquer qu'avec la passerelle d'accès distant via une connexion *IPsec* chiffrée et authentifiée (*full tunneling*).

j) **[ELEVE]** La solution de chiffrement des disques des postes nomades doit être qualifiée par l'ANSSI au niveau standard et utilisée conformément aux conditions figurant dans la décision de qualification.

k) **[ELEVE]** Les flux entre les postes nomades et les passerelles doivent être chiffrés à l'aide de solutions de chiffrement et d'authentification IPsec qualifiées par l'ANSSI au niveau standard et utilisées conformément aux conditions figurant dans la décision de qualification.

IV.5.14. Développement et sécurité des logiciels

Les exigences du présent chapitre sont applicables à l'ensemble des logiciels contribuant aux traitements permettant l'acquisition et la vérification des données d'identification, la constitution du dossier de preuve et l'envoi du résultat de la vérification d'identité au service métier.

a) Le logiciel doit faire l'objet de revues régulières du code[14].

b) Le logiciel doit faire l'objet de tests de non-régression avant mise en production d'une nouvelle version.

c) Le logiciel doit faire l'objet d'un parcours de recettes documenté pour chaque version devant être mise en production.

d) Le logiciel doit générer des journaux d'enregistrement adaptés pour la corrélation des enregistrements entre les différents processus du service.

e) Le développeur du logiciel doit être sensibilisé aux risques spécifiques liés au domaine de la vérification d'identité, et être tenu à une obligation de discrétion.

f) Le développement du logiciel doit être réalisé dans des conditions permettant une un enregistrement des actions de chaque développeur et une consultation à des fins d'audit.

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

IV.5.15. Gestion des incidents

a) Il est recommandé que le prestataire de vérification d'identité à distance mette en place un processus de gestion de crise en cas d'incident de sécurité majeur affectant le service de vérification d'identité à distance.

b) Le prestataire de vérification d'identité à distance doit informer l'ANSSI sans délai, conformément à [PROCESS_CERTIF_SERVICE] et [PROCESS_QUALIF_SERVICE] en cas d'incident affectant ou susceptible d'affecter le service de vérification d'identité à distance.

IV.6. Organisation du prestataire et gouvernance

IV.6.1. Recrutement

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

b) Le prestataire doit mettre en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté de ses personnels. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions[15]. Ces vérifications doivent être menées préalablement au

[14] Voir les différents guides de l'ANSSI sur les règles de programmation pour le développement sécurisé: https://www.ssi.gouv.fr/administration/bonnes-pratiques

[15] En droit français, l'employeur peut demander à ses personnels la présentation d'une copie du bulletin n°3 de leur casier judiciaire. L'employeur peut décider en cas de refus de présenter cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

recrutement et revues régulièrement (le délai entre deux revues ne doit pas excéder trois ans). Les opérateurs, et les référents fraude doivent être liés contractuellement avec le prestataire.

c) Le prestataire doit, après le recrutement, sensibiliser les opérateurs et référents fraude aux risques spécifiques relatifs à leur fonction, et les informer de leur obligation de discrétion

IV.6.2. Charte d'éthique

a) Le prestataire doit disposer d'une charte d'éthique intégrée au règlement intérieur, prévoyant notamment que :

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

b) Le prestataire doit faire signer à l'ensemble de son personnel la charte d'éthique prévue à l'exigence IV.6.2.a) et préalablement à la réalisation de la prestation.

c) Le prestataire doit veiller au respect de la charte d'éthique et prévoir des sanctions disciplinaires à l'intention des opérateurs, des administrateurs et des experts du service de vérification ayant enfreint les règles de sécurité ou la charte d'éthique.

IV.6.3. Organisation et gestion des compétences

a) Le prestataire doit employer un nombre suffisant d'opérateurs et de référents fraude assurant les missions et disposant des compétences identifiées en Annexe 2 pour assurer totalement et dans tous ses aspects le service de vérification d'identité à distance.

b) Le prestataire doit mettre à disposition des opérateurs et des référents fraude l'ensemble du matériel pédagogique et technique qui leur permettent de remplir les missions qui leurs sont confiées.

c) Le prestataire doit élaborer et mettre en œuvre un plan de formation régulier des opérateurs et des référents fraude en adéquation avec les missions et compétences identifiées en Annexe 2.

d) Le prestataire doit élaborer et mettre en œuvre un plan de contrôle régulier afin de vérifier que les opérateurs et référents fraude disposent des compétences identifiées en Annexe 2.

e) Le prestataire doit prévoir que chaque opérateur et référent fraude, préalablement à la réalisation de la prestation, a bien suivi le plan de formation et réussi le plan de contrôle.

IV.6.4. Bulletins opérationnels

a) Le prestataire doit mettre en place des bulletins opérationnels et y faire figurer, depuis le dernier bulletin opérationnel, au minimum :

- les indicateurs opérationnels du service (exigence IV.7.1.b) ;
- une revue des réclamations (exigences du chapitre IV.3.1.4) 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 (exigences IV.2.5g) et IV.5.15b)) ;

- la date de la dernière exécution du plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité (exigences du chapitre IV.2.5) ;
- les taux de faux négatifs (FRR) et de faux positifs (FAR) pour la vérification de l'authenticité du titre d'identité mesurés lors de la dernière exécution du plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité (exigences du chapitre IV.2.5) ;
- les taux de faux négatifs (FRR) et de faux positifs (FAR) pour la comparaison du visage de l'utilisateur mesurés lors de la dernière exécution du plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité (exigences du chapitre IV.2.5) ;
- les taux de faux négatifs (FRR) et de faux positifs (FAR) pour la détection du vivant mesurés lors de la dernière exécution du plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité (exigences du chapitre IV.2.5) ;
- une revue des éventuelles modifications apportées :
    - au système d'information du service de vérification d'identité à distance,
    - à l'appréciation des risques relatifs à l'usurpation d'identité (exigences du chapitre IV.2.2) notamment si la liste des scénarios de risque a été modifiée,
    - à l'appréciation des risques relatifs à la sécurité des systèmes d'information (exigences du chapitre IV.2.3) notamment si la liste des scénarios de risque a été modifiée,
    - au plan de traitement des risques (exigences du chapitre IV.2.4),
    - à la politique de vérification d'identité à distance (exigences du chapitre IV.3),
    - à la déclaration des pratiques de vérification d'identité à distance (exigences du chapitre IV.3),
    - à la politique de sécurité des systèmes d'information (exigences du chapitre IV.5.2),
    - au plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité (exigences du chapitre IV.2.5).

b) Le prestataire doit transmettre au commanditaire, à la fréquence définie dans la convention de service, les bulletins opérationnels relatifs au service de vérification d'identité à distance.

Il est recommandé que le prestataire transmette les bulletins opérationnels tous les mois.

c) Le prestataire doit assurer la confidentialité des bulletins opérationnels.

IV.6.5. Relations avec les services de l'État

a) Le prestataire doit nommer un officier de sécurité chargé notamment d'assurer la liaison avec les services de l'État compétents en cas de fraude ou d'attaque.

IV.7. Qualité et niveau de service

IV.7.1. Qualité du service

a) Le prestataire doit élaborer et mettre en œuvre un processus de capitalisation des incidents et fraudes détectés afin d'améliorer continuellement l'efficacité de son service de vérification d'identité à distance.

b) Le prestataire doit définir avec le commanditaire les indicateurs opérationnels du service de vérification d'identité à distance.

c) Le prestataire doit au minimum mettre en place les moyens de mesurer les indicateurs opérationnels suivants :

- le temps moyen, minimal et maximal d'attente des utilisateurs ;

- le nombre de vérifications d'identité à distance réalisées ;
- le nombre de vérifications d'identité à distance selon le verdict (succès ou échec) ;
- le nombre de vérifications d'identité à distance pour lesquelles le service a prononcé un verdict « échec », selon le motif de l'échec ;
- le nombre de vérifications d'identité à distance pour lesquelles le service a prononcé un verdict « échec » au motif qu'une usurpation d'identité était suspectée ou avérée, selon la nature de la tentative d'usurpation d'identité[16] ;
- le nombre de vérifications d'identité à distance pour lesquelles le service a prononcé un verdict « succès » et qui se sont révélées être a postériori des usurpations d'identité, selon que l'usurpation a été détectée par le prestataire ou par le commanditaire ;
- le nombre des réclamations reçues, en cours de traitement ou clôturées ;
- le temps moyen, minimal et maximal de clôture des réclamations.

d) Le prestataire doit élaborer et tenir à jour un processus de mesure des indicateurs décrivant, pour chacun des indicateurs opérationnels (exigence IV.7.1.b), les méthodes et moyens mis en œuvre par le prestataire pour mesurer l'indicateur.

IV.7.2. Convention de service

IV.7.2.1. Modalités de la prestation

a) La convention de service établie entre le prestataire et le commanditaire doit décrire l'organisation, le périmètre et les objectifs de la prestation de vérification d'identité à distance.

b) La convention de service doit décrire les moyens techniques et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation.

c) La convention de service doit préciser 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 commanditaire.

d) La politique de vérification d'identité à distance doit être annexée à la convention de service.

IV.7.2.2. Organisation du service

a) La convention de service doit stipuler que le prestataire désigne en son sein un interlocuteur auprès du commanditaire en charge d'assurer le suivi opérationnel de la prestation.

b) La convention de service doit stipuler si le prestataire autorise l'accès à distance d'une part de son personnel au système d'information du service de vérification d'identité à distance.

IV.7.2.3. Localisation

a) La convention de service doit décrire la localisation du traitement et du stockage des données relatives au service de vérification d'identité à distance pour ce commanditaire, notamment les données relatives aux utilisateurs.

IV.7.2.4. Responsabilités

a) La convention de service doit stipuler que le prestataire ne débute la prestation qu'après approbation formelle et écrite par le commanditaire de la convention de service.

[16] Pour identifier la nature d'une tentative d'usurpation d'identité, il est recommandé que le prestataire s'appuie sur les scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité identifiée au chapitre IV.2.2.

b) La convention de service doit stipuler que le prestataire informe le commanditaire de tout manquement à la convention de service.

c) La convention de service doit stipuler que le prestataire informe le commanditaire en cas d'incident de sécurité détecté sur le système d'information du service de vérification d'identité à distance, et préciser les modalités et le délai maximal pour transmettre les informations relatives à l'incident de sécurité au commanditaire.

d) La convention de service doit stipuler que le prestataire ne réalise que des actions strictement en adéquation avec les objectifs de la prestation.

e) La convention de service doit stipuler que le prestataire enregistre automatiquement comme réclamation (voir exigences du chapitre IV.3.1.4) toutes les vérifications d'identité à distance pour lesquelles le prestataire a prononcé un verdict « succès » et le commanditaire suspecte ou a détecté une usurpation d'identité.

f) La convention de service doit stipuler que le commanditaire déclare remplir toutes les obligations légales nécessaires à la prestation et notamment celles relatives à la collecte, au traitement et au transfert des données à caractère personnel et aux traitements biométriques. La convention de service doit spécifier les finalités de ces collectes, traitements et transferts, et identifier le cadre réglementaire applicable.

g) La convention de service doit définir les responsabilités et les mesures prises respectivement par le prestataire et le commanditaire pour réduire les risques potentiels relatifs à la prestation, notamment ceux en matière d'usurpation d'identité, de collecte et de traitement des données à caractère personnel.

h) La convention de service doit stipuler que le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés au service métier et notamment à son système d'information dans le cadre de sa prestation, préciser la couverture de l'assurance et inclure l'attestation d'assurance.

i) La convention de service doit préciser les mesures mises en œuvre par le prestataire au titre de son plan d'arrêt d'activité.

IV.7.2.5. Confidentialité et protection de l'information

a) La convention de service doit stipuler que le prestataire ne collecte et ne traite que les données, adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

b) La convention de service doit stipuler que le prestataire ne divulgue aucune donnée relative aux utilisateurs à des tiers, sauf autorisation formelle et écrite du commanditaire, et en accord avec la réglementation en matière de protection des données à caractère personnel [RGPD].

c) La convention de service doit préciser les clauses relatives à l'éthique du prestataire et inclure la charte d'éthique du prestataire.

d) La convention de service doit préciser les modalités d'accès, de stockage, de transport, de reproduction, de destruction et de restitution des données relatives à ce commanditaire, notamment celles relatives aux utilisateurs.

IV.7.2.6. Lois et réglementations

a) La convention de service doit être rédigée en français. Le prestataire peut fournir une traduction de courtoisie de la convention de service si le commanditaire en fait la demande.

b) La convention de service doit stipuler que seule la version française fait foi, notamment dans le cadre d'un litige.

c) La convention de service doit préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation et réglementation applicable notamment celle relative à la protection des données à caractère personnel [RGPD].

d) La convention de service doit préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité.

e) La convention de service doit préciser que la législation applicable à la convention de service est la législation française.

IV.7.2.7. Sous-traitance

a) La convention de service doit préciser que le prestataire peut si nécessaire sous-traiter tout ou partie de la prestation à un autre prestataire, ci-après le « sous-traitant », sous réserve que l'ensemble des conditions énoncées ci-dessous soient respectées :

- il existe une convention de service entre le prestataire et le sous-traitant ;
- le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire ;
- le sous-traitant respecte les exigences du présent référentiel.

IV.7.2.8. Livrables

a) La convention de service doit définir les livrables attendus dans le cadre de la prestation, les règles de titularité et les niveaux de sensibilité relatifs à ces livrables, ainsi que les modalités de protection associées.

b) La convention de service doit préciser que les livrables de la prestation sont en langue française sauf si le commanditaire en fait la demande formelle et écrite.

IV.7.2.9. Niveau de service

a) La convention de service doit identifier les indicateurs opérationnels permettant de mesurer le niveau de service de la prestation (exigences du chapitre IV.6.4).

b) La convention de service doit identifier la fréquence à laquelle le prestataire transmet au service métier les bulletins opérationnels (exigences du chapitre IV.6.4).

c) La convention de service doit stipuler que le prestataire définit et met en œuvre un processus d'amélioration continue de l'efficacité du service de vérification d'identité à distance s'appuyant notamment sur les indicateurs opérationnels.

d) La convention de service doit identifier les plages horaires opérationnelles du service de vérification d'identité à distance.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

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. Disponible sur https://www.eur-lex.europa.eu
[RGPD]	Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) Disponible sur https://www.eur-lex.europa.eu
[RGS]	Référentiel général de sécurité, faisant l'objet du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives Disponible sur http://www.legifrance.gouv.fr
[DECRET_2015-350]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur http://www.legifrance.gouv.fr
[DECRET_2020-118]	Décret n°2020-118 du 12 février 2020 renforçant le dispositif national de lutte contre le blanchiment de capitaux et le financement du terrorisme. Disponible sur http://www.legifrance.gouv.fr
[II_910]	Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, 22 octobre 2013. Disponible sur http://www.legifrance.gouv.fr
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur http://www.legifrance.gouv.fr
[CPCE]	Code des postes et des communications électroniques, version en vigueur Disponible sur http://www.legifrance.gouv.fr

II. Normes et documents techniques

Renvoi	Document
[ADMIN_SEC]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, référence ANSSI-PA-022, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[EBIOS_RM]	Ebios Risk Manager, ANSSI, 2018. Disponible sur http://www.ssi.gouv.fr
[CC_CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version en cours. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version 2.03. Disponible sur http://www.ssi.gouv.fr
[CRYPTO_B2]	Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques. Disponible sur http://www.ssi.gouv.fr

Renvoi	Document
[CRYPTO_B3]	Règles et recommandations concernant les mécanismes d'authentification, ANSSI. Disponible sur http://www.ssi.gouv.fr
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'Hygiène Informatique, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[MIE]	Référentiel d'exigences de sécurité, Moyens d'dentification électronique, ANSSI, version en vigueur.
[NT_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[INTERCO_INTERNET]	Recommandations relatives à l'interconnexion d'un système d'information à Internet, ANSSI, référence ANSSI-PA-066, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[ISO27002]	Norme internationale ISO/IEC 27002:2013 : Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information. Disponible sur http://www.iso.org
[ISO27005]	Norme internationale ISO/IEC27005:2011 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information. Disponible sur http://www.iso.org
[ISO30107-3]	Norme internationale ISO/IEC 30107-3. Technologies de l'information — Détection d'attaque de présentation en biométrie — Partie 3: Essais et rapports d'essai. Disponible sur http://www.iso.org
[NOMADISME]	Recommandations sur le nomadisme numérique, ANSSI, référence ANSSI-PA-054, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[ARCHI_DR]	Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte, ANSSI, référence ANSSI-PG-075, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[SecNumCloud]	Prestataires de services d'informatique en nuage (SecNumCloud), ANSSI, référentiel d'exigences, version 3.1 du 11 juin 2018. Disponible sur http://www.ssi.gouv.fr
[CNIL_Guide_conservation]	Guide pratique – Les durées de conservation, CNIL, version en vigueur. Disponible sur https://www.cnil.fr

III. Autres références documentaires

Renvoi	Document
[PROCESS_QUALIF_SERVICE]	Processus de qualification d'un service, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[PROCESS_QUALIF_PRODUIT]	Processus de qualification d'un produit, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[PROCESS_CERTIF_SERVICE]	Processus de certification des services, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr

Annexe 2 Missions et compétences du personnel du prestataire

IV. Opérateur

IV.1. Missions

L'opérateur doit assurer les missions suivantes :

a) vérifier, conformément à la politique de vérification d'identité à distance, l'identité des utilisateurs sur la base des données d'identification relatives aux utilisateurs acquises et des résultats des traitements automatisés réalisés sur ces données d'identification ;

b) si le service est de type « synchrone avec interaction humaine », formuler aux utilisateurs, dans la langue retenue, des demandes dans le cadre des étapes d'acquisition et de vérification des données d'identification (ex. : luminosité, mise au point, retrait des lunettes de l'utilisateur, etc.) conformément à la politique de vérification d'identité à distance ;

c) prononcer le verdict « succès » ou « échec » de la vérification d'identité à distance[17].

d) générer une alerte à chaque suspicion ou détection d'une usurpation d'identité.

IV.2. Compétences et connaissances

L'opérateur doit disposer des compétences suivantes :

a) connaitre et appliquer la politique de vérification d'identité à distance ;

b) connaitre et appliquer la politique de sécurité des systèmes d'information ;

c) connaître l'état de la menace relative à l'usurpation d'identité ;

d) connaitre et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment le [RGPD] ;

e) connaitre les modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité ;

f) être physionomiste, reconnaitre et comparer des visages sur des supports photographiques et vidéo ;

g) connaître les éléments de sécurité des titres d'identité ainsi que les vérifications à réaliser pour identifier de titres d'identité falsifiés ou altérés ;

h) connaître et maîtriser l'utilisation du registre PRADO[18].

V. Référent fraude Titre d'identité

V.1. Missions

Le référent fraude Titre d'identité doit assurer les missions suivantes :

a) valider formellement les modifications de la politique de vérification d'identité à distance lorsque ces modifications sont relatives aux titres d'identité ;

[17] Conformément à l'exigence IV.3.3.2.o), lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité, le verdict de la vérification d'identité à distance prononcé par le service est automatiquement « échec » », sans intervention d'un opérateur, si les traitements automatisés relatifs à la vérification de l'authenticité du titre d'identité concluent que le titre n'est pas authentique.

[18] Voir acronyme au chapitre I.3.1.

b) [lorsque l'authenticité du titre d'identité est vérifiée de manière cryptographique à l'aide du composant de sécurité] valider la conception et l'implémentation de la fonction de vérification de l'authenticité du titre d'identité ;

c) [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] traiter les alertes générées par les opérateurs lorsqu'ils suspectent ou détectent un scénario de risque identifié dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant les titres d'identité ;

d) [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] traiter les alertes générées lorsqu'un opérateur a proposé un verdict de la vérification d'identité à distance « succès » alors que les traitements automatisés suspectent ou détectent une fraude relative au titre d'identité ;

e) [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] assurer la formation des opérateurs aux vérifications relatives aux titres d'identité, et notamment aux contrôles des éléments de sécurité des titres d'identité afin d'identifier les titres d'identité falsifiés ou altérés ;

f) [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] assurer la formation des opérateurs aux modes opératoires des attaquants permettant d'aboutir aux scénario de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant les titres d'identité ;

g) [lorsque l'authenticité du titre d'identité n'est pas vérifiée de manière cryptographique à l'aide du composant de sécurité] contrôler que les opérateurs disposent des compétences attendues au chapitre IV.2 et relatives aux titres d'identité.

V.2. Compétences et connaissances

Le référent fraude Titre d'identité doit disposer des compétences suivantes :

a) connaitre et appliquer la politique de vérification d'identité à distance ;

b) connaitre et appliquer la politique de sécurité des systèmes d'information ;

c) maitriser l'état de la menace relative aux titres d'identité falsifiés ou altérés ;

d) connaitre et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment le [RGPD] ;

e) **[SUBSTANTIEL]** connaître l'état de la menace relative à l'usurpation d'identité ;

f) **[SUBSTANTIEL]** maîtriser les modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant les titres d'identité ;

g) **[SUBSTANTIEL]** maîtriser les éléments de sécurité des titres d'identité ainsi que les vérifications à réaliser pour identifier les occurrences des scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant les titres d'identité ;

h) **[SUBSTANTIEL]** connaître et appliquer les procédures relatives aux alertes générées par un opérateur lorsqu'il suspecte ou détecte une usurpation d'identité mettant en œuvre un titre d'identité falsifié ou altéré ;

i) **[SUBSTANTIEL]** connaître et appliquer les procédures relatives aux alertes générées lorsqu'un opérateur propose un verdict de la vérification d'identité à distance à « succès » alors que les traitements automatisés suspectent ou détectent une fraude relative au titre d'identité.

VI. Référent fraude Biométrie

VI.1. Missions

Le référent fraude Biométrie doit assurer les missions suivantes :

a) traiter les alertes générées par les opérateurs lorsqu'ils suspectent ou détectent une occurrence d'un scénario de risque identifié dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant la biométrie ;

b) traiter les alertes générées lorsqu'un opérateur a proposé un verdict de la vérification d'identité à distance à « succès » alors que les traitements automatisés suspectent ou détectent une fraude relative à la biométrie ;

c) assurer la formation des opérateurs aux vérifications relatives à la biométrie, et notamment à la vérification des données d'identification biométriques, à la comparaison de visages ;

d) assurer la formation des opérateurs aux modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant la biométrie ;

e) contrôler que les opérateurs disposent des compétences attendues au chapitre IV.2 et relatives à la biométrie ;

f) valider formellement les modifications de la politique de vérification d'identité à distance lorsque ces modifications sont relatives à la biométrie ;

g) valider la conception et l'implémentation des vérifications relatives à la biométrie réalisées par traitement automatisé.

VI.2. Compétences et connaissances

Le référent fraude Biométrie doit disposer des compétences suivantes :

a) connaitre et appliquer la politique de vérification d'identité à distance ;

b) connaitre et appliquer la politique de sécurité des systèmes d'information ;

c) connaître l'état de la menace relative à l'usurpation d'identité ;

d) maîtriser l'état de la menace relative à la biométrie ;

e) connaître et appliquer la législation et la réglementation en vigueur relative à la protection des données à caractère personnel, et notamment [RGPD] ;

f) maîtriser les modes opératoires des attaquants permettant d'aboutir aux scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant la biométrie ;

g) maîtriser les vérifications à réaliser pour identifier les occurrences des scénarios de risque identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité et concernant la biométrie ;

h) connaître et appliquer les procédures relatives aux alertes générées par un opérateur lorsqu'il suspecte ou détecte une occurrence d'un scénario de risque identifié dans l'appréciation des risques et relatif à la biométrie ;

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

Annexe 3 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI aux commanditaires.

a) Le commanditaire peut, lorsqu'il est une autorité administrative ou un opérateur d'importance vitale ou de service essentiel, demander à l'ANSSI de participer à la définition du cahier des charges faisant l'objet d'un appel d'offres ou d'un contrat.

b) Il est recommandé que le commanditaire désigne parmi ses personnels un référent opérationnel chargé d'être l'interlocuteur privilégié avec le prestataire concernant le fonctionnement du service de vérification d'identité à distance.

c) Il est recommandé que le commanditaire identifie dans la convention de service les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

d) Il est recommandé que le commanditaire exige du prestataire que la fréquence des bulletins opérationnels devant être définie dans la convention de service soit mensuelle.

e) Il est recommandé que le commanditaire notifie au prestataire toutes les vérifications d'identité à distance pour lesquelles le prestataire a prononcé un verdict « succès » et le commanditaire suspecte ou a détecté une usurpation d'identité. Conformément à la convention de service, le prestataire enregistre automatiquement ces notifications comme réclamations et les traite comme telles.

f) Il est recommandé que le commanditaire mette en place un processus de gestion de crise en cas d'incident de sécurité majeur affectant le prestataire.

Annexe 4 Titres d'identité acceptés

Seuls les titres d'identité suivants sont acceptés dans le cadre du présent référentiel, sous réserve qu'ils présentent des caractéristiques permettant de répondre aux exigences définies dans le présent référentiel :

a) Pour les Français, les ressortissants des autres 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 en France ou dans un autre 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 selon le 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 dispensés de l'obligation de visa de court séjour ne résidant 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, sous réserve que le pays émetteur mette à disposition les moyens nécessaires à la vérification de la validité du titre. Si la dispense 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 autorité pour le pays concerné.

d) Pour les ressortissants de pays tiers réfugiés ou reconnus apatrides ou 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, à un statut uniforme pour les réfugiés ou les personnes pouvant bénéficier de la protection subsidiaire, et au contenu de cette protection, le passeport est remplacé par le titre de voyage délivré par l'État qui a reconnu la qualité de réfugié ou d'apatride ou accordé la protection.