Politique du service vérification d'identité à distance PVID Docaposte

OID : 1.3.6.1.4.1.50034.1.3.1

Historique des évolutions

Date	Version	Rédigé par	Modification
01/03/2021	v1.0	CSC	Rédaction initiale
15/11/2021	v1.1	AGA	Mise à jour des langues
15/12/2021	v1.2	VRE	Relecture / modifications mineures
23/08/2023	V1.3	CSC	Modifications mineures / mise en forme
31/03/2025	V1.4	AL/VRE	Changement de gouvernance, suppression paragraphe traitements automatique concernant la biométrie et ajout de la référence à la PGSSI Docaposte.

Table des matières

1. Introduction

1.1 Présentation Générale

AR24 est une société de services informatiques commercialisant des services de confiance dont notamment un service de vérification d'identité par face à face vidéo à distance. Ce service existe depuis plusieurs années et a historiquement été construit afin d'être utilisé au sein du service d'envoi recommandé électronique Qualifié d'AR24. La portée de ce service n'est désormais plus limitée à ce seul usage et ce service a vocation à être certifié par l'ANSSI dans le cadre du référentiel PVID.

L'organisation adoptée pour cela est présentée dans la section 1.4

La présente Politique définit les engagements d'AR24 dans le cadre de la fourniture de service d'identification à distance.

1.2 Identification du document

La présente politique est identifiée par l'OID suivant : 1.3.6.1.4.1.50034.1.3.1

1.3 Date d'entrée en vigueur

La présente politique entre en vigueur le : 03/04/2025

1.4 Gestion de la politique

1.4.1 Entité gérant la politique

La politique est gérée par les membres du comité de pilotage d'AR24.

Le membres du comité de pilotage sont les membres du CODIR et la politique est revue lors des séances CODIR hebdomadaires.

1.4.2 Point de contact

AR24 SAS
45-47 Boulevard Paul Vaillant Couturier

94200 IVRY-SUR-SEINE

Ou

ar24.contact@docaposte.fr

1.4.3 Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par les membres du comité de pilotage ou les personnes désignées par celui-ci. Cette relecture a pour objectif d'assurer :

- La conformité de la politique avec les exigences réglementaires et normatives portant sur la fourniture d'un service de vérification d'identité à distance certifié au titre du référentiel PVID
- La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par AR24 et ses partenaires
- Que toute modification importante dans la fourniture du service de vérification d'identité à distance fasse l'objet d'une information de l'ANSSI selon les modalités décrites dans les procédures de qualification.

1.4.4 Amendements à la politique

AR24 contrôle que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.

1.4.4.1Procédure d'amendement

Hormis les corrections induites par les audits ou des corrections mineures (erreurs, oublis, précisions, etc.), les amendements pressentis à la présente politique portent sur :

- Un éventuel changement du niveau de garantie
- Des changements d'ordre technique (mise en œuvre, partenaires / fournisseurs, etc.)

Avant tout changement effectif du service (passage en production), AR24 réalise une analyse d'impact afin de déterminer si les évolutions ont une incidence sur la conformité de l'offre qualifiée et si celle-ci est majeure (impliquant un changement d'OID). L'analyse d'impact peut, à cette occasion, être soumise à l'ANSSI et à l'organisme de certification pour avis ou commentaire.

Le cas échéant, la politique est mise à jour, approuvée et publiée avant toute mise en œuvre. Les Conditions Générales d'Utilisation du service son amendées concomitamment si besoin.

1.4.4.2 Mécanisme et période d'information sur les amendements

AR24 adressera annuellement à l'ANSSI et à l'organisme de certification une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

En cas de changement de la présente politique ou des CGU, les utilisateurs clients en sont avertis par un message dans leur espace dédié.

1.4.4.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de la présente politique ayant un impact majeur sur le service se traduit par une évolution de l'OID afin que les utilisateurs puissent clairement distinguer quelles vérifications d'identités correspondent à quelles exigences.

1.5 Documents associés

1.5.1 Conditions générales d'utilisation

Les CGU applicables (et leurs version antérieures) sont disponibles sur le site d'AR24.

1.5.2 Documents normatifs

[ANSSI_PVID] https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf

[HYGIENE] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

[NOMADISME] https://www.ssi.gouv.fr/uploads/2018/10/guide_nomadisme_anssi_pa_054_v1.pdf

[NT_ADMIN] https://www.ssi.gouv.fr/uploads/2018/04/anssi-guide-admin_securisee_si_v3-0.pdf

[RGPD] https://www.cnil.fr/fr/reglement-europeen-protection-donnees

1.6 Entités intervenant dans le service de vérification d'identité

1.6.1 Prestataire de vérification d'identité

Le PVID est AR24.

1.6.2 Opérateur du service de vérification d'identité à distance

L'opérateur du service de vérification d'identité à distance est AR24.

1.6.3 Utilisateurs

Les utilisateurs sont les personnes physiques qui procèdent à la vérification de leurs identités sur le service.

1.6.4 Clients

Les clients sont des organismes qui font appel au service de vérification d'identité pour vérifier l'identités de leurs utilisateurs. Les interactions des clients se font par API ou par une interface d'administration mise à disposition par AR24.

1.7 Responsabilités concernant la mise à disposition des informations devant être publiées

1.7.1 Entités chargées de la mise à disposition des informations

La mise à disposition des informations devant être publiées à destination des utilisateurs et clients du service est réalisée par l'équipe en charge du site internet https://www.ar24.fr

1.7.2 Informations devant être publiées

AR24 s'engage à publier au minimum les informations suivantes à destination des utilisateurs du services :

- Le présent document, décrivant la politique du service de vérification d'identité à distance
- Les conditions générales d'utilisation du service

1.7.3 Délais et fréquence de publication

Les informations liées au service (nouvelle version des présentes, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de AR24. En particulier, toute nouvelle version est communiquée aux clients et, le cas échéant, faire l'objet d'un nouvel accord.

Les systèmes publiant ces informations sont au moins disponibles les jours ouvrés.

Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

AR24 met à disposition sur ces sites les moyens nécessaires à la vérification d'intégrité des informations publiées.

1.7.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de AR24, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe et d'un deuxième facteur d'identification.

2. Généralités

2.1 Présentation du service

Le service d'identification à distance AR24 est un service de type hybride asynchrone. Il est donc composé de deux étapes : une phase de capture des données d'identification puis une phase de traitement au terme de laquelle un opérateur humain prononce un verdict binaire (succès ou échec) pour la vérification d'identité.

La phase de capture se déroule de la manière suivante :

- L'utilisateur sélectionne le titre d'identité qu'il va utiliser pour s'identifier (seuls les titres d'identités acceptés par le service figurent parmi les choix proposés)
- L'utilisateur présente ce titre d'identité à sa caméra, une vidéo du titre est ainsi capturée (si le titre dispose d'un recto et d'un verso cette séquence est exécutée pour chacune des faces du titre), la capture du titre intègre un facteur non-prédictible
- L'utilisateur présente son visage à la camera
- L'utilisateur effectue une ou des actions spécifiques non-prédictibles afin de répondre au besoin de détection du vivant

La phase de traitement se déroule de la manière suivante :

<u>Traitement automatisé :</u>

- Le traitement automatisé du titre d'identité afin :
  - .1 D'en extraire le contenu textuel et d'effectuer un contrôle de cohérence automatisé
  - .2 Contrôle visant à déterminer l'authenticité du titre
- Des traitements automatisés optionnels peuvent être effectués. Ces traitements peuvent porter sur :
  - .1 La comparaison faciale entre la ou les photos extraites du titre d'identité et le visage présenté lors de la phase de capture
  - .2 Des contrôles visant à détecter l'édition ou la falsification numérique (deepfakes)
  - .3 La détection de la bonne réalisation des challenges non-prédictibles

Traitements manuels :

Les opérateurs du service procèdent aux vérifications suivantes :

- Vérification de l'authenticité du titre d'identité :
  - .1 Le titre est dans un état physique acceptable
  - .2 Le titre ne présente pas de modification visible
  - .3 Le titre est authentique (il ne s'agit pas d'une contrefaçon)
- Comparaison du visage de la personne : le visage présent sur le titre est le même que le visage présent sur la vidéo de capture du visage
- Contrôle du vivant : l'utilisateur effectue correctement l'action non-prédictible demandée lors de la phase de capture

A ces fins l'opérateur dispose des outils suivants :

- Accès à un fichier de titre interne basé sur le fichier PRADO et d'autres sources d'informations agrégées
- L'affichage, sous forme d'indicateur, des résultats des contrôles automatisés effectués précédemment
- Un outil permettant de zoomer sur les titres
- Un outil permettant de lire les vidéos issues de la phase de capture
- Des indications automatisées liées au risque de fraude de la vérification en cours
- Un système d'alerte à utiliser lors de la détection d'activité suspecte
- Un système d'escalade permettant d'effectuer des levées de doutes

2.2 Titre d'identité

La liste des titres d'identités acceptés par le service est disponible en annexe.

Les attributs du titre d'identité qui caractérisent l'unicité de l'identité d'une personne physique sont :

- Les noms et prénoms de la personne
- Le numéro du document
- La date et le lieu de naissance
- Nationalité
- Civilité

Le service peut retourner des données complémentaires lorsque le service métier en fait la demande, ces données complémentaires peuvent être :

- Une photo du titre d'identité extraite de la vidéo du titre issue de la phase de capture
- Une photo du visage de l'utilisateur extrait de la vidéo issue de la phase de capture
- Des données variables renseignées par le service métier lors de la création de la demande du contrôle. Il n'y a pas de limitation particulière sur ces données mais si elles contiennent des données personnelles, le service métier s'assure du bon respect de la règlementation sur les données personnelles.

Les données complémentaires susmentionnées n'entrent pas dans le calcul du verdict de la vérification d'identité à distance.

2.2.1 Fraude

Les indicateurs permettant de détecter les tentatives d'usurpation d'identité relatives aux scénarios de risques identifiés dans l'appréciation des risques relatifs à l'usurpation d'identité sont les suivants :

- Incohérence sur le contrôle de données du titre d'identité
- Soumission d'une pièce d'identité d'une personnalité publique
- Nouvelle tentative de fraude après une fraude identifiée
- Analyses avancées sur les soumissions
- Résultats issus de contrôles automatiques
- Résultats issus de contrôles manuels

Chaque usurpation d'identité suspectée ou avérée détectée par le service AR24 ou par le service métier implique la génération d'une alerte qui est relayée auprès de tous les référents du service.

Les voies de recours offertes aux utilisateurs du service pour toute demande et plus spécifiquement en cas de demande d'annulation d'une identification frauduleuse ou en cas de verdict défavorable lors de l'identification d'un utilisateur de bonne foi sont les suivantes :

- Par courriel à l'adresse ar24.contact@docaposte.fr
- Par le biais du site AR24 depuis le lien mis à disposition des utilisateurs lors des parcours utilisateurs

2.2.2 Données à caractère personnel

2.2.2.1Alternative à la vérification d'identité à distance

Le service ne propose pas d'alternative à la vérification d'identité à distance. Les services métiers sont libres de fournir des alternatives dans leurs parcours.

2.2.2.2 Listes des données personnelles

AR24 respecte le principe de minimisation des données personnelles collectées et conservées et ne traite donc que des données qui sont nécessaires (qu'elles soient exigées par la réglementation ou indispensable à la bonne tenue du parcours d'identification).

Les données à caractères personnelles traitées par le service sont stockées pendant la durée de conservation du dossier de preuve et sont les suivantes :

Données transmises par le service métier :

- L'adresse courriel de l'utilisateur
- Les données complémentaires peuvent comporter des données personnelles

Données extraites du titre d'identité

- La vidéo du titre d'identité recto verso le cas échéant (peut faire l'objet d'un traitement biométrique)
- Une photo du titre d'identité extraite de la vidéo susmentionnée (peut faire l'objet d'un traitement biométrique)
- La ou les photos de l'utilisateur présentes sur le titre d'identité
- Le numéro de document du titre d'identité
- Le nom de naissance de l'utilisateur
- Le nom d'usage (marital)
- Les prénoms de l'utilisateur
- La nationalité de l'utilisateur
- La civilité de l'utilisateur
- La date et le lieu de naissance de l'utilisateur

Données extraites de la vidéo du visage :

- La vidéo du visage de l'utilisateur (peut faire l'objet d'un traitement biométrique)
- Une photo du visage de l'utilisateur extrait de la vidéo susmentionnée (peut faire l'objet d'un traitement biométrique)

Données stockées sous forme d'image :

- La photo de la face du titre d'identité
- La photo du verso du titre

La finalité principale de conservation des données à caractère personnel relatives aux utilisateurs et traitées par le service de vérification a pour but de répondre aux exigences du référentiel PVID et au principe de responsabilisation du responsable de traitement. La sous finalité du traitement de données biométriques limité à 96h après acquisition des données, sur acceptation, est l'amélioration du service.

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

L'accès aux données 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 est interdit.

2.2.3 Langages

Les langues supportées par le service de vérification d'identité à distance sont les suivantes :

- Le Français
- L'Anglais

- Le Néerlandais

Le choix de la langue est proposé à l'utilisateur avant le début de la phase d'acquisition des données.

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 avant la phase d'acquisition.

2.2.4 Enregistrement et traitement des réclamations

AR24 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.

Ce processus fonctionne de la manière suivante :

- Le demandeur formule et transmet sa demande à AR24 à l'adresse ar24.contact@docaposte.fr ou en suivant le lien proposé lors du parcours de vérification
- AR24 accuse réception de la demande et indique un temps de réponse maximum pour l'acceptation de la demande, passer ce délai maximum la demande est considérée comme refusée implicitement et ne sera pas traitée
- AR24 indique si la demande sera traitée ou non et indique un délai maximum de traitement en cas de réponse favorable
- AR24 communique le résultat du traitement de la réclamation au demandeur

2.3 Acquisition

2.3.1 Terminal

L'acquisition des données d'identification relatives aux utilisateurs est réalisée par le terminal de l'utilisateur.

L'installation d'une application n'est pas requise. L'acquisition des données s'effectuent par un navigateur internet. Le terminal doit disposer d'une caméra de résolution minimum de 720 x 1280 points.

2.3.2 Titres d'identité

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

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

- Indication concernant la position du titre dans le champ de capture
- Indication de luminosité trop faible
- Indication de reflet / éviter les sources de lumières directes sur le titre
- Indication sur la distance du titre par rapport à la camera
- Indication qu'aucun document n'est détecté

2.3.3 Visage

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

Les demandes qui peuvent être formulées par le service à l'utilisateur pour une acquisition correcte du visage sont automatisées et peuvent-être les suivantes :

- Indication concernant la position du visage
- Indication concernant la distance du visage par rapport à la camera
- Indication de luminosité trop faible / contre-jour
- Demande de retrait des lunettes

2.4 Vérification

2.4.1 Terminal

Certains contrôles peuvent être effectués sur le terminal de l'utilisateur toutefois aucun contrôle réalisé sur le terminal de l'utilisateur ne peut contribuer au verdict « succès » de la vérification d'identité à distance.

2.4.2 Titres d'identité

2.4.2.1 Titres d'identité acceptés

La liste des titres d'identité acceptés est disponible en annexe.

Pour chacun des titres d'identité accepté le service nomme au moins un référent fraude Titre d'identité compétent. La liste des référents fraudes pour chacun des titres est maintenue au sein du registre interne de gestion des titres du service.

Seuls les titres non-expirés sont acceptés par le service. S'il existe une extension de validité officielle pour un titre d'identité particulier, le service pourra appliquer cette extension.

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

En cas de non-validité du titre le verdict de la vérification d'identité à distance est systématiquement « échec ».

La résolution minimale après compression de la vidéo du titre d'identité acceptée par le service ne doit pas être inférieur à 720p, soit 1280 x 720 à 25 images par seconde.

2.4.2.2 Titres altérés physiquement

Les titres altérés physiquement font l'objet d'un traitement particulier afin de s'assurer que :

- Aucune information n'est indisponible du fait de l'altération du document
- L'altération est le résultat d'une usure normale et ne semble pas avoir été provoquée délibérément
- L'altération ne masque pas ou n'empêche pas le contrôle d'éléments de sécurité unique
- En cas d'éléments de sécurité répétitifs, l'altération ne doit pas empêcher le contrôle d'au moins l'un d'entre eux

2.4.3 Comparaison du visage

La résolution minimale après compression de la vidéo du visage de l'utilisateur acceptée par le service est de 720p soit 1280 × 720 à 25 images par seconde.

2.5 Dossier de preuve

Chaque vérification d'identité dont le verdict est prononcé fait l'objet de la création d'un dossier de preuve.

Les éléments intégrés au dossier de preuve sont les suivants :

- Les données d'identification :
  - La vidéo 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 à la suite de 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.

Le dossier de preuve ne contient aucune donnée ayant pour finalité un traitement biométrique

En cas de verdict *succès* la durée de conservation des dossiers de preuve est fixée en tenant compte de la durée pendant laquelle peut survenir un contentieux et donc en fonction de l'activité du service métier à l'origine de la demande de vérification d'identité et au maximum 10 ans. En cas de verdict *échec* le dossier de preuve est conservé pendant trois mois.

2.5.1 Sécurité

Les dossiers de preuves sont chiffrés à l'aide de clés AES 256 protégées sur les serveurs sécurisés du service. Les dossiers de preuve sont conservés sur un système de stockage hors-ligne. Chaque dossier de preuve est chiffré avec une clé unique.

Aucun administrateur ne dispose simultanément de l'accès aux clés et au dispositif de stockage. L'accès en lecture doit donc se faire en présence de plusieurs administrateurs.

2.5.2 Accès

Les utilisateurs peuvent exercer leur droit d'accès aux données à caractères personnel les concernant présentes dans le dossier de preuve toutefois les utilisateurs ne peuvent pas exercer de droit de rectification sur ce dossier.

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

2.6 Transmission du résultat

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

2.6.1 Contenu du résultat

Le résultat de la vérification d'identité à distance n'est constitué que :

- Du verdict (succès ou échec) de la vérification
- Du motif de refus le cas échéant
- Des attributs d'identité relatifs à l'utilisateur suivants :
    - 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
    - Date d'émission du titre
    - Pays d'émission du titre
    - Date d'expiration du titre
    - Nationalité
    - MRZ
    - Type du document
- Les éventuelles données complémentaires transmises ou demandées par le service métier (ces données ne sont pas utilisées dans l'élaboration du verdict)
    - Date de la soumission de la vérification d'identité par l'utilisateur à l'issue de la phase de capture
    - Date de traitement de la vérification d'identité par un opérateur

Le résultat ne contient aucun autre élément et ne contient pas de score issu des vérifications.

Les vidéos du titre d'identité et du visage de l'utilisateur ne sont en aucune manière transmises au service métier (ni totalement ni partiellement).

2.6.2 Délai de transmission

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 est de quatre-vingt-seize heures.

2.7 Qualité et niveau de service

2.7.1 Qualité de service

AR24 met en œuvre un processus d'amélioration continue de son service notamment en capitalisant sur les incidents et les fraudes détectés.

AR24 définit avec le service métier les indicateurs opérationnels du service de vérification d'identité à distance, ces indicateurs sont au moins les suivants :

- Le temps moyen, minimal et maximal d'attente des utilisateurs ;
- Le nombre de vérifications d'identité à distance réalisées ;
- Le nombre de vérifications 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 ;
- 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.

AR24 maintient un registre indiquant pour chacun de ces indicateurs de quelle manière sont effectués les mesures et le processus de mesure associé.

2.7.2 Convention de service

AR24 établit une convention de service avec chacun des services métiers qui souhaite faire appel au service de vérification d'identité. Cette convention de service contient au moins les éléments exigés par le référentiel PVID et peut être annexé à un contrat.

2.7.3 Bulletins opérationnels

AR24 met en place des bulletins opérationnels qui sont communiqués mensuellement (sauf mention contraire dans la convention de service) à chaque commanditaire. Ces bulletins contiennent les informations suivantes :

Informations spécifiques au commanditaire :

- Les indicateurs opérationnels du service
- Une revue des réclamations reçues, en cours de traitement et clôturées

Informations génériques (communiquées à tous les commanditaires) :

- Une revue des incidents de sécurité relatifs à la sécurité des systèmes d'information
- Une revue des incidents de sécurité notifiés à l'ANSSI
- La date de la dernière exécution du plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité
- 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
- 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
- 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
- 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 notamment si la liste des scénarios de risque a été modifiée
    - À l'appréciation des risques relatifs à la sécurité des systèmes d'information notamment si la liste des scénarios de risque a été modifiée
    - Au plan de traitement des risques
    - À la politique de vérification d'identité à distance
    - À la déclaration des pratiques de vérification d'identité à distance
    - À la politique de sécurité des systèmes d'information
    - Au plan de test de la capacité effective du service à détecter des tentatives d'usurpation d'identité

Les bulletins opérationnels sont communiqués au commanditaire par un moyen qui permet d'en assurer la confidentialité.

3. Protection de l'information et gestion des risques

3.1Appréciation des risques

Avant le lancement du service qualifié, AR24 effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques et commerciaux. L'analyse de risque identifie, en particulier, les systèmes « critiques » du service.

Les mesures de sécurité seront prises en tenant compte du résultat de cette analyse.

AR24 est sujet, par la PGSSI du groupe Docaposte, les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en œuvre les mesures identifiées.

L'analyse de risques est examinée et révisée annuellement. Elle est aussi mise à jour à chaque modification ayant un impact important sur le service, notamment en cas de modification des politiques ou pratiques relatives à sa fourniture.

Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

3.2 PGSSI

En tant que filiale du groupe Docaposte, AR24 est soumis à la Politique Générale de Sécurité des Systèmes d'Information (PGSSI) du groupe Docaposte, qui a été approuvée par la direction Docaposte. La PGSSI d'après sa classification ne peut pas être communiquée aux abonnés du service. Mais la politique pourra être communiquée aux prestataires, aux organismes d'évaluation, à l'ANSSI et aux employés de AR24 s'ils souhaitent la consulter.

AR24 conserve la responsabilité globale de la conformité avec les procédures prévues dans la PGSSI du groupe.

En particulier, l'entreprise doit s'assurer de la mise en œuvre effective des mesures prévues dans les Politiques Opérationnelles de Sécurité (POS).

Pour cela AR24, s'assure de vérifier l'applicabilité de ces mesures car certaines mesures ne peuvent pas s'appliquer à l'entité d'AR24. La revue des POS sera intégrée au processus de revue de sécurité du système d'information afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité du groupe.

La configuration du SI est régulièrement auditée afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité.

L'évolution et les changements de la PGSSI sont revu annuellement.

.

3.3 Homologation

À la suite de la finalisation de l'analyse de risque, AR24 procèdera à l'homologation du service. Cette homologation est réalisée préalablement à la fourniture du service puis révisée au moins tous les deux ans.

3.4 Territorialité du service

L'hébergement et le traitement des données relatives au service de vérification d'identité à distance ainsi que l'administration et l'exploitation du service s'effectuent exclusivement au sein du territoire d'un Etat membre de l'Union Européenne.

3.5 Niveau de sécurité

AR24 applique l'ensemble des règles du niveau standard du guide d'hygiène informatique de l'ANSSI au système d'information du service de vérification d'identité à distance.

3.5.1 Opérateurs

Les opérateurs disposent d'accès restreints au strict nécessaire à la réalisation de leurs missions.

3.6 Terminal

La confidentialité et l'intégrité des données d'identification échangées entre le terminal et le service de vérification d'identité à distance est assurée par une communication chiffrée.

3.7 Plan de contrôle

AR24 élabore et met 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

Le plan de contrôle est révisé 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.

Le plan de traitement des risques est mis à jour à l'issue de l'exécution du plan de contrôle afin d'y intégrer les résultats.

Les résultats du contrôle sont validés formellement et par écrit par la direction.

3.8 Accès au SI

3.8.1 Contrôle d'accès

AR24 met en œuvre un contrôle d'accès aux systèmes d'information du service de vérification d'identité à distance.

Des procédures de gestion des habilitations sont mises en œuvre, prenant en compte les différents rôles identifiés par la présente politique. Ces procédures assurent que l'octroi et le retrait des habilitations s'effectuent en accord avec la gestion des ressources humaines.

Tout utilisateur doit être identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service.

Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

L'accès aux logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est restreint et contrôlé.

Les informations sensibles sont protégées contre la divulgation résultant de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.

La PGSSI décrit en détail les règles de contrôle d'accès applicables au SI du service.

3.8.2 Sécurité physique

Les accès aux locaux hébergeant le système d'information du service de vérification d'identité à distance sont nominatifs et limités aux personnes autorisées et strictement nécessaires à l'exploitation du service.

Un contrôle physique de ces accès est en place, est auditable et la liste du personnel autorisé est contrôlée lors des revues périodiques d'habilitation.

Les journaux d'accès sont conservés de manière à garantir leur confidentialité et ne sont accessibles qu'au personnel nécessaire. Ces journaux sont protégés en intégrité par un horodatage électronique.

3.8.3 Accès distant

AR24 permet l'accès distant à certains composant du SI notamment afin de répondre au risque pandémique.

L'objectif d'AR24 est de respecter l'intégralité des recommandations du guide du nomadisme édité par l'ANSSI. AR24 maintient un registre dans lequel il est indiqué quelles mesures sont en place afin de répondre aux recommandations respectées et quelles sont les justifications pour les mesures non respectées.

AR24 met en place une passerelle dédiée aux accès distants.

Les postes nomades utilisés sont dédiés à leur usage nécessaire à la prestation de vérification d'identité à distance. Les postes d'administrateurs nomades peuvent être utilisés pour administrer d'autres services qualifiés dont les conditions de sécurité sont identiques.

3.8.3.1 Sécurité des postes nomades

L'authentification sur les postes nomades se fait au minimum par deux facteurs.

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

L'usage de support amovible sur les postes nomades n'est pas autorisé.

Les disques des postes nomades sont intégralement chiffrés grâce à des mécanismes conformes à [CRYPTO_B1].

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

3.9 Journalisation

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 sont journalisés dans un composant du système d'information du service auquel les opérateurs et les référents fraude ne disposent d'aucun accès.

3.10 Sauvegardes

AR24 élabore et met en œuvre un plan de sauvegarde et de restauration des dispositifs du service de vérification d'identité à distance, comportant :

- Sauvegarde des systèmes
- Sauvegarde des configurations
- Sauvegarde des données
- Sauvegarde des dossiers de preuves (hors-ligne)

AR24 définit dans le plan de sauvegarde et met en œuvre des mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes.

Le plan de sauvegarde et de restauration est testé au moins une fois par an.

3.11 Cloisonnement du système d'information du service

AR24 élabore et maintient à jour une description détaillée de l'architecture du système d'information du service de vérification d'identité à distance.

Cette description comprend 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.

AR24 met en place un filtrage de tous les flux aux interconnexions du système d'information du service de vérification d'identité à distance.

3.12 Administration et exploitation du service

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

Si un accès internet est nécessaire ce dernier se fait par un poste de travail physique ou virtuel distinct et déployé au sein d'une zone externe au système d'information du service de vérification d'identité à distance.

3.13 Interconnexions avec le service métier

AR24 met en place une authentification mutuelle auprès du service métier lors de la transmission des résultats. AR24 met également en place des mécanismes visant à garantir l'intégrité, la confidentialité et l'impossibilité de rejouer des données transmises.

3.14 Développement et sécurité des logiciels

AR24 dispose d'un processus de revue de code et de tests de non-régression avant mise en production. Pour cela un parcours de recette est documenté et réalisé avant chaque mise en production.

Les modifications du code source sont consignées dans un outil interne de gestion de version et l'auteur de chaque modification est identifié.

Chaque composante logicielle génère des journaux d'enregistrement permettant la corrélation avec d'autres processus du service.

Le personnel qui intervient sur le développement du produit est sensibilisé aux risques spécifiques liés au domaine de la vérification d'identité et est formé aux bonnes pratiques de sécurité liées au développement logiciel.

3.15 Gestion des incidents

AR24 dispose d'un processus de gestion de crise en cas d'incident de sécurité majeur affectant le service de vérification d'identité à distance. Ce processus intègre une notification à l'ANSSI sans délai en cas d'incident majeur affectant ou susceptible d'affecter le service de vérification d'identité à distance.

4. Gestion et exploitation du service d'identification à distance

4.1 Organisation interne

L'organisation du service en assure la fiabilité. Les objectifs et mesures pour assurer cette fiabilité sont décrites dans le présent chapitre.

4.1.1 Rôles de confiance

Les rôles de confiance identifiés sont les suivants :

- **Responsable sécurité** : Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère notamment les contrôles d'accès physiques aux équipements des systèmes sensibles.
- **Administrateur système** : Personnes chargées de la mise en route, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations…). Elles assurent l'administration technique des systèmes et des réseaux de la composante, ainsi que leur surveillance (détection d'incident).
- **Opérateur de vérification d'identité** : Les opérateurs sont les personnes en charge d'effectuer les vérifications d'identité
- **Référent fraude Titre d'identité**
- **Référent fraude Biométrie**

AR24 nomme un officier de sécurité chargé d'assurer la liaison avec les services de l'Etat en cas de fraude ou d'attaque, ce rôle est attribué au RSSI.

4.1.2 Séparation des tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Responsable sécurité et administrateur système
- Administrateur système et opérateur de vérification d'identité ou référent fraude

4.2 Ressources humaines

4.2.1 Charte d'éthique

AR24 dispose d'une charte d'éthique signée par l'ensemble du personnel.

4.2.2 Qualifications, compétences et habilitations requises

AR24 s'assure de la compétence et de l'adéquation des personnels employés. AR24 s'assure d'employer un nombre suffisant d'opérateurs et de référents fraude pour répondre à ses engagements de qualité et de sécurité.

4.2.3 Procédures de vérification des antécédents

AR24 met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté du personnel qu'il emploie. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

À ce titre, AR24 peut demander la communication d'une copie du bulletin n° 3 du casier judiciaire et peut décider, en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

Par ailleurs, AR24 vérifie l'absence de conflit d'intérêt avant toute attribution d'un rôle de confiance.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

AR24 vérifie également la véracité de curriculum vitae préalablement à l'embauche ou à l'attribution du rôle de confiance.

4.2.4 Relation contractuelle

Les opérateurs et les référents fraude sont liés contractuellement avec AR24.

4.2.5 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter.

Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

4.2.6 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions. Le personnel suit une formation spécifique traitant des nouvelles menaces et des nouvelles pratiques de sécurité au moins tous les 12 mois.

Les opérateurs de vérification d'identité et les référents fraude bénéficient d'une formation spécifique à leurs missions et un plan de contrôle régulier est en place afin de vérifier qu'ils disposent des compétences nécessaires.

Préalablement à l'attribution effective d'un rôle de confiance, l'opérateur ou le référent fraude suit le plan de formation et le plan de contrôle avec succès.

4.2.7 Sanctions en cas d'actions non autorisées ou non-respect des règles

En cas de non-respect des obligations, procédures ou exigences exprimées dans la présente politique ou la PGSSI du service ou de la charte d'éthique, le personnel s'expose à des sanctions disciplinaires telles que prévu dans le règlement intérieur de la société.

4.2.8 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux ou sur les composantes du service est soumis aux exigences de la présente section (4.2). Cela apparaît dans des clauses spécifiques dans les contrats avec ces prestataires.

En particulier, la PGSSI du service est transmise aux prestataires externes.

4.2.9 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il intervient.

4.3 Gestion des biens

4.3.1 Généralités

Un inventaire des biens est réalisé et tenu à jour dans le cadre de l'analyse de risques du service. Les biens sont gérés en adéquation avec leur classification, telle que déterminée par celle-ci.

4.3.2 Supports

Les supports sont gérés en adéquation avec leur classification, telle que déterminée par celle-ci.

4.4 Sécurité physique et environnementale

4.4.1 Situation géographique et construction des sites

Les conditions d'hébergement des équipements sur lesquelles reposent la sécurité et la continuité du service permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

4.4.2 Accès physique

Pour les systèmes critiques du service, l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Des mesures sont mises en œuvre afin de prévenir la perte ou l'altération des biens nécessaires au bon fonctionnement du service, ou la perte ou le vol d'informations.

4.4.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

4.4.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

4.4.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

4.4.6 Conservation des supports

Les différentes informations intervenant dans les activités du service sont identifiées, et leurs besoins de sécurité, définis (en confidentialité, intégrité et disponibilité). AR24 maintient un inventaire de ces informations et met en place des mesures pour en éviter la compromission et le vol.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période durant laquelle AR24 s'engage à conserver les informations qu'ils contiennent.

4.4.7 Mise hors service des supports

En fin de vie, les supports sont détruits ou réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations qu'ils contiennent.

4.5 Sécurité opérationnelle

4.5.1 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque.

4.5.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques permettent de remplir au minimum les objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non- autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

4.5.1.2 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système contribuant au service est documentée et respecte, dans la mesure du possible, des normes de modélisation et d'implémentation. La configuration des composantes du service, ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

AR24 garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

AR24 utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

AR24 met en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, dès la conception des produits et des services, en veillant notamment à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

4.5.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'une composante du système est signalée à l'entité identifiée en 1.4.1 pour validation. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée et est conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

4.5.3 Évaluation des vulnérabilités

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 2 mois après leur publication. Dans tous les cas, une analyse d'impact est réalisée afin de déterminer l'opportunité de les appliquer ; si un correctif n'est pas appliqué, l'analyse en justifie la décision.

Dans le cas de vulnérabilités « critiques » (CVSS≥9), l'analyse d'impact est effectuée dans les 48 heures suivant la publication de la vulnérabilité.

4.5.4 Horodatage / Système de datation

Plusieurs exigences de la présente politique nécessitent la datation par les différentes composantes des événements liés aux activités du service.

Pour dater ces évènements, les différentes composantes du service recourent à l'utilisation de l'heure système, en assurant une synchronisation quotidienne de celle-ci, au minimum à la minute près, et par rapport à une source fiable de temps UTC.

4.6 Sécurité réseau

Le réseau et ses systèmes sont protégés contre les attaques. En particulier,

a) Le SI est segmenté en réseaux ou zones en fonction de l'analyse des risques, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services. Les mêmes contrôles de sécurité sont appliqués à tous les systèmes partageant la même zone.
b) L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du SI du service. AR24 garantit que les composants du réseau local (routeurs, etc.) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique ; des dispositifs de surveillance (avec alarme automatique) de ces configurations sont mis en place.
c) Tous les systèmes critiques sont isolés dans une ou plusieurs zones sécurisées.
d) L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne doivent pas être utilisés à d'autres fins. Les systèmes de production du service sont séparés des systèmes utilisés pour le développement et les tests.
e) La communication entre des systèmes de confiance distincts n'est établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.
f) Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par TSP, est effectuée par une personne ou une entité ayant les compétences, les outils, le code de déontologie et l'indépendance nécessaires. Cette analyse doit donner lieu à un rapport.
g) Un test d'intrusion sur les systèmes du service est réalisé lors de la mise en place et après toute évolution majeure de l'infrastructure ou des applications.

4.6.1 Tests d'intrusion

AR24 archive les rapports des tests d'intrusion et s'assure que ces derniers sont réalisés par des personnes dont les compétences, les outils, l'éthique et l'indépendance permet la production d'un rapport fiable.

4.7 Gestion des incidents et supervision

Les activités du système concernant l'accès aux systèmes informatiques, l'utilisation des systèmes informatiques et les demandes de service sont surveillées.

AR24 réagit de manière coordonnée afin de répondre rapidement aux incidents et de limiter l'impact des violations de la sécurité. La responsabilité d'assurer le suivi des alertes sur les événements de sécurité

potentiellement critiques et de veiller à ce que les incidents pertinents soient signalés conformément aux procédures est attribuée à des personnels de confiance.

Les procédures de déclaration et d'intervention d'incident minimisent les dommages causés par les incidents de sécurité et les dysfonctionnements.

4.7.1 Procédures de remontée et de traitement des incidents et des compromissions

AR24 notifie à l'ANSSI, dans un délai maximal de 24 heures après en avoir eu connaissance, tout atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Lorsque le manquement à la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, AR24 informe sans délai la personne physique ou morale concernée.

4.8 Gestion des traces

4.8.1 Type d'événements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du service, chaque entité en opérant une composante doit au minimum journaliser les événements décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création, modification, suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
- Démarrage et arrêt des systèmes informatiques et des applications
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises à la suite d'une défaillance de la fonction de journalisation
- Connexion et déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

Les accès physiques	Contrôle d'accès au centre de données Enregistrement vidéo de l'accès à la salle d'hébergement

Les actions de maintenance et de changements de la configuration des systèmes	Tracés par les intervenants dans l'outil de gestion
Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs…).	Tracés dans le cadre des procédures de gestion interne

Chaque enregistrement d'un événement dans un journal contient au minimum les champs suivants :

- Type de l'événement
- Nom de l'exécutant ou référence du système déclenchant l'événement
- Date et heure de l'événement
- Résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.

De plus, en fonction du type de l'événement, chaque enregistrement contient également les champs suivants :

- Destinataire de l'opération
- Nom du demandeur de l'opération ou référence du système effectuant la demande
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes)
- Cause de l'événement
- Toute information caractérisant l'événement

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture est faite, sauf exception, le même jour ouvré que l'événement. Les événements et données spécifiques à journaliser sont documentés par AR24.

4.8.2 Fréquence de traitement des journaux d'événements

Chaque composante du service est en mesure de détecter toute tentative de violation de son intégrité.

Les journaux d'événements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec, les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles est périodiquement effectué afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

4.8.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins 1 (un) mois.

4.8.4 Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'événements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'événements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des événements respecte les exigences de la présente politique.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

4.8.5 Procédure de sauvegarde des journaux d'événements

Chaque composante du service met en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux.

4.8.6 Notification de l'enregistrement d'un événement au responsable de l'événement

Aucune exigence spécifique.

4.9 Continuité d'activité

4.9.1 Reprise à la suite de la compromission et sinistre

Chaque entité opérant une composante du service met en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement AR24. Le cas de l'incident majeur est impérativement traité dès détection et traité dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé…). AR24 prévient directement et sans délai l'ANSSI.

Si l'un des algorithmes, ou des paramètres associés, utilisés par le service ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors AR24 :

- En informe tous les utilisateurs et tiers impactés
- Le cas échéant, révoque les identifiants concernés.

4.9.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)

Chaque composante du service dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente politique et des documents associés.

Ce plan est testé annuellement.

4.9.3 Capacités de continuité d'activité à la suite d'un sinistre

Les différentes composantes du service disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente politique.

4.10 Fin d'activité

AR24 a provisionné les moyens financiers nécessaires à la fin d'activité (y compris au frais de notification des entités concernées).

En cas de fin d'activité du service, AR24 s'engage à informer les clients avec un préavis d'au minimum un mois. Durant cette période, la création de nouvelle demande de vérification ne sera plus possible.

AR24 déposera les dossiers de preuve chez un tiers archiveur afin de rester disponibles à des fins de justice durant la durée prévue. L'ensemble des obligations d'AR24 seront transférées soit au tiers archiveur, soit à un tiers sous contrat.

Les obligations transférées comprendront au moins les points suivants :

- Les dossiers de preuves doivent être conservés au moins pendant la durée prévue
- Les données personnelles ne pourront être exploitée à d'autres fins que celles mentionnées dans la présente politique

AR24 informera ses utilisateurs, ses sous-traitants et les tiers de l'arrêt d'activité.

Le contact identifié sur le site de l'ANSSI (https://www.ssi.gouv.fr) est immédiatement informé en cas de cessation d'activité du service.

5. Autres problématiques métiers et légales

5.1 Responsabilité financière

5.1.1 Couverture par les assurances

AR24 a contracté une assurance Responsabilité Civile Professionnelle. AR24 est assuré contre :

- Toutes les conséquences pécuniaires,
  - Résultant de tout fondement en responsabilité civile,
  - Lui incombant dans l'exercice de l'ensemble de ses activités (définies à l'article 3 des conditions particulières),
- À raison de tous dommages (corporels, matériels et immatériels),
  - Dans le monde entier, sous réserve des dispositions de l'article 2.2 des conventions spéciales,
  - Quelle que soit la juridiction qui les apprécie,
  - Dès lors que le risque n'est pas expressément visé dans une des exclusions (article 1.4 des conventions spéciales).

- Sont notamment couvertes les conséquences des risques suivants, spécifiques au secteur les nouvelles technologies :
  - Faute, erreur, omission, négligence, inobservation des règles de l'art, défaut de conseil (inadéquation entre la solution proposée et les besoins du client, spécifications insuffisantes)
  - Obligation de résultat
  - Engagement de performance et de délai
  - Dysfonctionnements (ex. bug)
  - Interruption de service dans les contrats d'hébergement (de données ou d'applicatif), d'infogérance ou de prestation en mode Saas ou l'équivalent
  - Inexécution partielle ou totale (ex : déni de service), mauvaise exécution d'une obligation contractuelle (ex : mauvaise conduite de projet)
  - Retard (même si la cause n'est pas accidentelle)
  - Atteinte aux droits de propriété intellectuelle et/ou industrielle (contrefaçon de brevets et droits d'auteurs, concurrence déloyale, parasitisme économique, etc.)
  - Divulgation d'information(s) confidentielle(s)
  - Engagements et modifications contractuels non formalisés par écrit (y compris cahier des charges)
  - Pertes de données clients et altérations ou destructions de biens confiés
  - Volet RC des Cyber Risques (virus, données personnelles, fraude informatique)
  - Volet Gestion de Crise des Cyber Risque
  - Acte(s) de malveillance / faute intentionnelle des salariés
  - Garantie de bonne fin et frais de retrait, remboursement des factures, pénalités de retard dans les marchés publics, frais de gestion des dossiers en crise

5.2 Couverture et garantie concernant les entités utilisatrices

Se référer aux sections afférentes au garanties pécuniaires décrites dans les *Conditions Générales d'Utilisation*.

5.3 Confidentialité des données professionnelles

5.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des clients et les pièces associées utilisées pour vérifier leur identité ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, etc.)

5.3.2 Responsabilités en termes de protection des informations confidentielles

AR24 respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, AR24 peut devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations à ses clients.

5.4 Protection des données personnelles

5.4.1 Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par AR24 et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier, la loi *Informatique et Libertés* et le *Règlement Général sur la Protection des Données* (RGPD).

5.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :

- Le cas échéant, les données d'identité des clients et les pièces associées utilisées pour vérifier leur identité ;
- Les adresses IP, *hostname* et les *UserAgents* des navigateurs utilisés par les clients pour accéder au service

5.4.3 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles transmises à AR24 par les utilisateurs du service ne doivent ni être divulguées, ni transférées à un tiers, sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Sur ce point, AR24 agit dans le respect de la législation et réglementation en vigueur sur le territoire français.

5.5 Obligations des utilisateurs

Les utilisateurs garantissent :

- Qu'ils ont pris connaissance de la présente politique
- Qu'ils ne présentent pas de fausses informations lors de la vérification de leur identité
- Qu'ils s'identifient de bonne foi et non dans un objectif fallacieux (usurpation d'identité d'un tier ou tentative de tromper le service)

5.6 Durée et fin anticipée de validité de la politique

5.6.1 Durée de validité

La présente politique reste en vigueur au moins un an après la dernière vérification d'identité effectuée.

5.6.2 Fin anticipée de validité

La publication d'une nouvelle version du référentiel PVID par l'ANSSI peut entraîner, en fonction des évolutions apportées, la nécessité pour AR24 de faire évoluer la présente politique.

5.6.3 Effets de la fin de validité et clauses restant applicables

Dans tous les cas, AR24 respectera les exigences réglementaires qui lui incombent.

5.7 Conformité aux législations et réglementations

Les pratiques de AR24 sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de AR24 prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur

infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (https://www.w3.org/Translations/WCAG20-fr/).

5.8 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

6. Liste des annexes

Annexe 1 : Liste des titres acceptés par le service