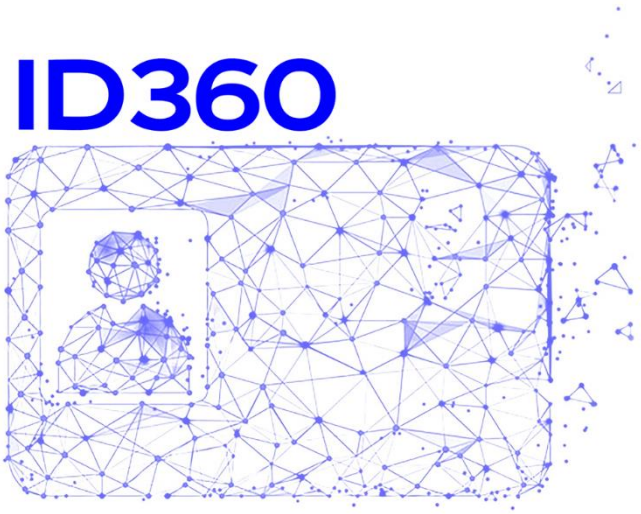

Politique et pratiques de service

ID360 : Service multimodal de vérification d'identité à distance

OID : 1.2.250.1.566.1.1.1.1.1

Version : 1.4.9

Date d'application : 01 Août 2022

Table des matières

I. Introduction

I.1. Présentation générale

Docaposte crée des solutions innovantes, personnalisées et durables pour permettre à toutes les organisations de réussir leur transformation numérique pour un avenir plus simple et serein.

ID360 est une solution conçue et proposée par Docaposte dans ce cadre, pour simplifier la gestion de l'identification et de l'authentification des Utilisateurs d'un service métier. ID360 est un service multimodal de vérification d'identité à distance, proposant un ensemble de méthodes permettant d'adresser différents niveaux de garantie.

Ce document constitue la politique et la déclaration de pratiques du service ID360 de vérification d'identité à distance proposé par Docaposte. Il expose les pratiques que Docaposte applique et s'engage à respecter dans le cadre de la fourniture de son service de vérification d'identité à distance. Cette politique identifie également les obligations et exigences portant sur les autres intervenants et sur les Utilisateurs du service.

Conscient des enjeux de sécurité inhérents à la nature du service ID360, Docaposte a fait certifier la conformité du service ID360 vis-à-vis de la norme ETSI EN 319 401, utilisée pour l'évaluation de l'ensemble des services de confiance qualifiés au titre du règlement eIDAS.

Le plan de ce document se conforme au chapitrage de la norme ETSI EN 319 401.

I.2. Identification du document

Ce document décrit la politique, et la déclaration de pratiques associées, identifiée par l'OID 1.2.250.1.566.1.1.1.1.1.

Ce document est identité par son titre et numéro de version tels que portés en page de garde.

I.3. Date d'entrée en vigueur

La politique et les pratiques décrites par ce document entrent en vigueur dès sa publication sur le site Docaposte.

I.4. Entités intervenant dans le service

I.4.1. Utilisateurs finaux

Les Utilisateurs finaux du service ID360 sont des personnes physiques désirant accéder à un service métier qui délègue à ID360 la vérification de leur identité préalablement à l'accès à une ressource de ce service métier.

Le service ID360 n'impose aucune contrainte sur la personne physique débutant un parcours de vérification d'identité en ligne. Chacune des modalités de vérification d'identité peut toutefois exiger certains justificatifs, dont elle est maître et seule à même d'en vérifier l'acceptabilité.

I.4.2. Services métier

Les services métier sont des services numériques, accessibles en ligne le plus souvent mais non exclusivement, qui demandent pour certains cas d'usage la vérification de l'identité de l'Utilisateur. Cette vérification d'identité peut répondre à des exigences règlementaires ou à des besoins fonctionnels propres.

Ces services métiers sont sous la responsabilité d'un commanditaire qui a contractualisé avec Docaposte afin de faire appel au service ID360 de vérification d'identité à distance. Le commanditaire fixe le niveau de confiance, les

modalités proposées et le parcours adaptés aux cas d'usage de chaque service métier dont il est responsable. Des administrateurs sont désignés par le commanditaire pour configurer le service ID360 selon ces besoins.

I.4.3. Modalités de vérification d'identité à distance

Les modalités de vérification d'identité à distance que peut proposer le service ID360 sont :

- Des services de vérification d'identité à distance certifiés par l'ANSSI sur la base du référentiel [PVID], au niveau substantiel ou élevé ; A ce jour, le service utilisé est le service de Docaposte AR24, dont l'OID est 1.3.6.1.4.1.50034.1.3.1 ;
- Des moyens d'identification électronique de niveau faible, substantiel ou élevé conformément au règlement d'exécution [RE 2015/1502], utilisés à travers FranceConnect ou FranceConnect+, ou directement proposés par le fournisseur d'identité émetteur ;
- D'autres modalités de vérification d'identité à distance sélectionnées par Docaposte.

I.5. Gestion de la politique

Docaposte est responsable, via un comité de pilotage du service, de la création, l'approbation, la maintenance et la modification de la politique et des pratiques des services. Le présent document est publié et communiqué au personnel et aux parties prenantes intéressées.

La Politique a vocation à être adaptée dans le temps pour refléter les modifications du service, suite à des évolutions des normes ou des réglementations applicables, ou à des choix techniques, fonctionnels ou d'organisation.

L'impact de chaque modification est systématiquement évalué par Docaposte. Toute modification significative du service, en particulier sur le niveau de sécurité du service ou de l'une de ses composantes, fait l'objet d'une nouvelle version de la politique et d'un changement de son OID. Cette nouvelle version est notifiée aux différentes parties prenantes avant son entrée en application, et avec, dans la mesure du possible, un délai de prévenance adéquat pour les adaptations qui pourraient être nécessaires.

I.6. Définitions

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 du système d'information – tout élément logiciel ou matériel constitutif du système d'information intervenant dans la fourniture du service d'identification 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.

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.

Données d'identification – ensemble de données à caractère personnel acquises et vérifiées par le service ID360 ou l'une de ses modalités afin de vérifier l'identité d'une personne physique.

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.

Dossier de preuve – élément conservé par le prestataire rassemblant a minima les données d'identification acquises, les informations résultant de la vérification d'identité réalisée ainsi que le résultat de la vérification d'identité à distance transmis au service métier. Le dossier de preuve ne contient aucune donnée biométrique.

Jeux de paramètres : Le service métier gère le paramétrage de la plateforme d'identification. Notamment, il définit les modalités acceptées pour la vérification d'identité à distance, mais aussi les preuves attendues, les parcours internes, etc.

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

Modalité : tout moyen, méthode, processus, permettant de vérifier l'identité ou d'authentifier un Utilisateur.

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

Niveau de garantie substantiel – un service de vérification d'identité à distance est dit de niveau de garantie substantiel lorsqu'il présente un niveau de garantie équivalent à une vérification d'identité réalisée en face à face physique par une personne formée ne disposant pas d'outillage (lampe ultraviolet, loupe, etc.) pour détecter de faux titres d'identité. Le profil d'attaquant considéré pour le niveau de garantie substantiel est toute personne, tout groupe de personnes ou toute organisation malveillante à l'exception des attaquants de type étatique, disposant d'un potentiel d'attaque modéré.

Opérateur – personnel du service de vérification d'identité à distance en charge de vérifier l'identité des Utilisateurs.

Résultat de la vérification d'identité à distance – élément 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 ainsi que les attributs d'identité relatifs aux Utilisateurs requis par le service métier. Le résultat de la vérification d'identité à distance ne contient aucune donnée biométrique.

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.

PVID : Modalité de vérification d'identité à distance, certifiée par l'ANSSI pour le niveau de garantie substantiel, qui a pour objectifs de réaliser l'acquisition et la vérification les données d'identification des Utilisateurs afin de les identifier et de transmettre le résultat de la vérification d'identité à distance au service ID360.

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 ID360.

SVID : Modalité de vérification d'identité à distance, non certifiée par l'ANSSI, qui a pour objectifs de réaliser l'acquisition et la vérification les données d'identification des Utilisateurs afin de les identifier et de transmettre le résultat de la vérification d'identité à distance au service ID360.

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 5 du présent référentiel.

Utilisateur – personne physique dont l'identité est vérifiée par le service de vérification d'identité à distance ID360.

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.

I.7. Documents associés

Référence	Document
[PVID]	Prestataires de vérification d'identité à distance - Référentiel d'exigences Version 1.1 du 1er mars 2021 https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel_exigences-pvid-v1.1.pdf
[eIDAS]	Règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23/07/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=FR
[RE 2015/1502]	Règlement d'exécution (UE) 2015/1502 de la Commission du 8/09/2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502
[RGPD]	Règlement Général sur la Protection des Données 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 (UE) 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) (europa.eu)

I.8. Acronymes

Acronyme	Signification
AIPD	Analyse d'impact relative à la protection des données
EBIOS	Expression des besoins et identification des objectifs de sécurité
ETSI	European Telecommunications Standards Institute
DPO	Data Protection Officer
LCB-FT	Lutte contre le blanchiment des capitaux et le financement du terrorisme
LCP	Lightweight Certificate Policy
MIE	Moyen d'identification électronique

PSSI	Politique de sécurité des systèmes d'information
RGPD	Règlement général sur la protection des données
RGS	Référentiel général de sécurité
SI	Système d'information

II. Service ID360

II.1. Présentation du service

II.1.1. Objectifs du service

ID360 est un service de vérification d'identité à distance, proposant un ensemble de méthodes permettant de répondre aux exigences de différents niveaux de garantie. L'acquisition et le contrôle de documents complémentaires peuvent être ajoutés optionnellement à la vérification d'identité.

Le service ID360 s'adresse à des fournisseurs de services métier, de tous types, devant procéder à la vérification d'identité à distance de leurs Utilisateurs.

ID360 propose une offre très large :

- ➔ ID360 répond à **de multiples enjeux dans différents domaines** :
  - Exigences légales : les niveaux de garantie les plus hauts de la vérification d'identité satisfont les besoins règlementaires définis pour l'entrée en relation dans le domaine bancaire par exemple, ou pour les services qualifiés au titre du règlement eIDAS,
  - Exigences de sécurité : les différents niveaux de garantie du service ID360 permettent de proposer à l'Utilisateur des modalités de vérification d'identité adaptées au risque évalué par le fournisseur du service métier, et donc aux contraintes minimales ;
  - Exigences métier : le fournisseur du service métier sélectionne les seules données d'identité dont il a besoin pour son service, et peut demander l'acquisition et le contrôle de documents complémentaires pertinents pour son activité.
- ➔ ID360 s'appuie sur **tout type de modalité de vérification d'identité à distance** :
  - Des moyens d'identification électronique certifiés ou notifiés au sens du règlement eIDAS, en particulier :
    - Les moyens d'identification électronique proposés sous FranceConnect ;
    - L'Identité Numérique de La Poste.
  - Des services de vérification d'identité en ligne, synchrones ou asynchrones, avec ou sans interaction avec un opérateur humain et :
    - Certifié conforme par l'ANSSI au référentiel PVID ;
    - Non certifiés par l'ANSSI, mais potentiellement certifiés selon d'autres référentiels et/ou conformes aux exigences règlementaires de LCB-FT ;
- ➔ ID360 adresse de **nombreux niveaux de garantie** :
  - Niveau de garantie eIDAS substantiel : des moyens d'identification électronique, notamment ceux sous FranceConnect+, et des services de vérification d'identité à distance de PVID peuvent proposer ce niveau ;
  - Niveau de garantie eIDAS faible : des moyens d'identification électronique, notamment ceux sous FranceConnect, peuvent proposer ce niveau ;
  - Autres niveaux bénéficiant ou non de certification, par exemple selon des normes ETSI relatives à la délivrance de certificats électronique.

ID360 propose à l'Utilisateur final les seules modalités de vérification d'identité configurées préalablement par le fournisseur du service métier selon son contexte et ses propres choix. ID360 prend en charge l'interfaçage technique avec les différentes modalités de vérification d'identité à distance et de renforcement d'authentification, et fournit au service métier les informations requises dans un format indépendant de la modalité utilisée. Lorsque la vérification d'identité a donné lieu à la génération d'une preuve vérifiable par les tiers, celle-ci est transmise en complément au service métier.

ID360 recueille des informations techniques et métier, archivées par le service à titre de preuve en cas de litige ou de suspicion d'usurpation d'identité.

II.1.2. Cinématique du service

Le parcours d'un Utilisateur final du service ID360 est le suivant :

- L'Utilisateur consomme un service métier qui requiert une vérification d'identité à distance ;
- Le service ID360 propose, selon la configuration du service métier, une ou plusieurs modalités de vérification d'identité à distance ;
- L'Utilisateur sélectionne l'une des modalités ;
- Le service ID360 redirige l'Utilisateur vers la modalité de vérification d'identité à distance sélectionnée ;
- L'Utilisateur suit les instructions propres à la modalité choisie pour faire vérifier son identité ;
- Le résultat de la vérification d'identité est produit par la modalité et retourné au service ID360 ;
- Le cas échéant, le service ID360 contrôle les documents complémentaires demandés par le client et fournis par l'Utilisateur ;
- Le service ID360 prépare un résultat standardisé de vérification d'identité à distance et le transmet au service métier ;
- Le service métier analyse le résultat obtenu et poursuit son traitement en conséquence.

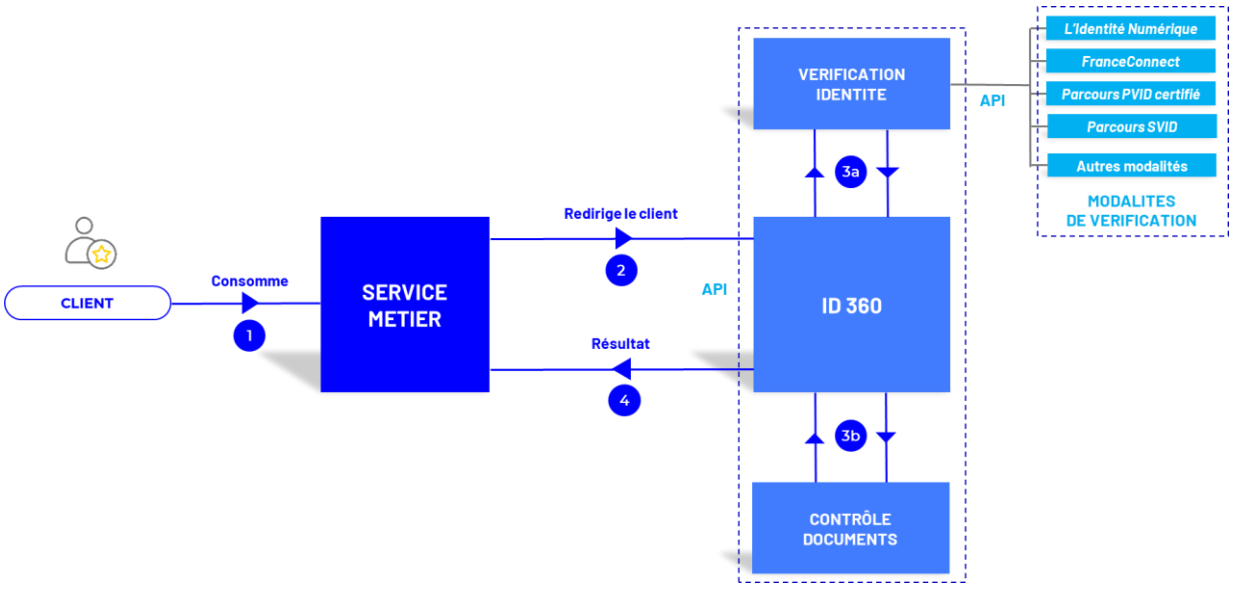

Figure 1 : Cinématique du service ID360

II.1.3. Niveaux de garantie de la vérification d'identité

Les exigences relatives à la vérification d'identité à distance sont distinctes selon le référentiel considéré (règlement eIDAS, RGS, normes ETSI, ...).

Le service ID360 se base en partie sur le règlement eIDAS pour définir les niveaux de garantie suivants :

- **Niveau élevé** (définition eIDAS): Ce niveau correspond à une vérification d'identité effectuée avec :
  - Un moyen d'identification électronique notifié au niveau Européen avec le niveau de garantie élevé (« High ») ou certifié par l'ANSSI conforme aux exigences du niveau de garantie élevé ;
  - Un service de vérification d'identité à distance certifié conforme par l'ANSSI aux exigences du référentiel [PVID] pour le niveau élevé ;
- **Niveau substantiel** (définition eIDAS): Ce niveau correspond à une vérification d'identité effectuée avec :
  - Un moyen d'identification électronique notifié au niveau Européen avec le niveau de garantie Substantiel (« Substantial ») ou certifié par l'ANSSI conforme aux exigences du niveau de garantie Substantiel ;

  - « Verif ID Certified » Un service de vérification d'identité à distance certifié conforme par l'ANSSI aux exigences du référentiel [PVID] pour le niveau Substantiel pour la France. Le service utilisé est le service de Docaposte AR24, dont l'OID est 1.3.6.1.4.1.50034.1.3.1 ;
  - Un processus reconnu comme équivalent au face-à-face physique avec présentation d'une pièce d'identité, conforme au niveau NCP/QCP de *l'ETSI EN 319411*.
- **Niveau renforcé** : Ce niveau correspond à une vérification d'identité effectuée avec :
  - « verif ID Secured » Un service de vérification d'identité à distance, effectuant la collecte du titre et du porteur, et les contrôles de validité et d'authenticité du titre d'identité, du porteur et de sa légitimité. Parcours non certifié par l'ANSSI, conforme au niveau LCP de *l'ETSI EN 319411,*
- **Niveau sécurisé** : Ce niveau correspond à une vérification d'identité effectuée avec :
  - Un moyen d'identification électronique notifié au niveau Européen avec le niveau de garantie Faible (« Low ») ou certifié par l'ANSSI conforme aux exigences du niveau de garantie Faible ou disponible sous FranceConnect ;
  - « Verif ID » Un service de vérification d'identité à distance, non certifié par l'ANSSI, paramétrable, effectuant les contrôles de validité et d'authenticité du titre d'identité, sans contrôles sur le porteur.

Note : pour les parcours « Verif ID » et « Verif ID Secured », la phase de collecte de documents d'identité peut être effectuée par le service métier ; le service ID360 effectue alors les contrôles sur ces documents et renvoie la réponse au service métier.

II.1.4. Collecte et contrôle de documents complémentaires

Le service ID360 peut, sur demande du service métier, collecter et contrôler des documents complémentaires, par exemple (liste non exhaustive) :

- Avis d'imposition ;
- Avis de taxes foncières ;
- Bulletin de salaire ;
- Justificatifs de domicile ;
- Relevé d'Identité Bancaire ;
- …

La liste des documents complémentaires traités par le service ID360 est fournie sur demande aux services métiers.

Les contrôles que le service ID360 peut effectuer sont :

- Des contrôles d'authenticité et/ou de validité du document ;
- Des contrôles sur le type de document présenté ;
- Des contrôles croisés avec les informations issues du titre d'identité (nom, prénom..);

ID360 propose différents outils ou services tiers pour obtenir des documents certifiés, selon les choix du service métier :

- Proposer à l'utilisateur d'utiliser les documents de son coffre-fort Digiposte s'il en dispose,

II.1.1. Acceptation préalable de termes

Le service ID360 peut, sur demande du service métier, présenter des termes (par exemple des Conditions Générales d'utilisation) du service métier à faire accepter par l'utilisateur. La trace de l'acceptation de ces termes est fournie au service métier et insérer dans le dossier de preuves.

Le service métier est responsable de ces termes, du contenu et de la version du document. ID360 conserve ainsi dans le dossier de preuve la version de ces termes.

II.1.2. Collecte et contrôle d'un attribut de contact

Le service ID360 peut, sur demande du service métier, collecter et contrôler un attribut de contact tel que le numéro de téléphone mobile ou l'adresse e-mail.

Le contrôle de cet attribut de contact consiste en l'envoi d'un code OTP via le canal indiqué ; l'Utilisateur est invité à saisir le code reçu afin de valider l'attribut.

II.1.3. Retour au service métier

Le résultat de la vérification d'identité est transmis au service métier dans tous les cas :

- Verdict d'échec ou de succès de la vérification d'identité ;
- Retour originel signé des modalités certifiées ou qualifiées,
- En cas de succès uniquement, des informations parmi :
    - Nom ;
    - Prénom ;
    - Genre ;
    - Date et lieu de naissance ;
    - Type et numéro du titre d'identité ;
    - Informations extraites des titres d'identité ;
    - Lieu de résidence ;
    - Adresse de messagerie ;
    - Numéro de téléphone ;
    - Images du titre d'identité;

- Selon la modalité, le détail des contrôles effectués et leur résultat.
- En cas de contrôle de documents complémentaires, pour chaque document :
    - Le type de document complémentaire demandé ;
    - Le document complémentaire collecté ;
    - Verdict de la vérification documentaire le cas échéant.
- (optionnellement) la trace d'acceptation des termes présentés
- (optionnellement) l'attribut de contact vérifié
- Le numéro d'archive du dossier de Preuve.

Le résultat ne contient aucun autre élément que ceux indiqués ci-dessus.

II.1.4. Paramétrage du service

Une interface d'administration est mise à disposition des administrateurs des services métier, leur permettant :

- la gestion de leurs opérateurs,
- la configuration de leurs jeux de paramètres
- la consultation des dossiers d'identification en cours.
- La déclaration de suspicion de fraude sur un dossier.

L'accès à l'interface d'administration est restreint à une personne habilitée du service métier avec un dispositif d'authentification renforcé à double facteur.

La configuration intègre notamment :

- La création d'« applications », permettant l'intégration d'ID360 dans plusieurs usages,
- La création de jeux de paramétrage, associés à une ou plusieurs applications, consistant à :
    - Sélectionner les modalités de vérification d'identité que le service métier souhaite présenter aux Utilisateurs, dans le cadre d'un usage,

- Pour les parcours paramétrables en ligne, sélectionner le niveau de contrôles souhaité,
- Sélectionner les modalités de renforcement d'authentification souhaitées,
- Sélectionner les éléments à retourner au service métier : image du titre d'identité, documents complémentaires,
- Sélectionner plusieurs options selon les choix précédents : contrôles d'authenticité des autres documents qu'identitaire, traitement en cas de rejet,...
- Paramétrer le visuel de la fenêtre du service ID360.

Chaque modification du paramétrage est journalisée et enregistrée.

Le choix d'une modalité qualifiée ou certifiée par l'ANSSI est soumis à un mode opératoire défini.

II.2. Dossier de preuve

Le service ID360 génère un dossier de preuve relatif à toutes les vérifications d'identité qu'il effectue pour le compte de ses clients.

Ce dossier de preuve est conservé par le service afin d'être utilisé :

- en cas de suspicion d'usurpation d'identité détectée par le service client ou par le fournisseur de la modalité de vérification d'identité ;
- en cas de litige ou de contestation concernant une vérification d'identité ;
- dans le cadre règlementaire du service métier ;
- sur requête judiciaire.

Les éléments de preuve conservés portent notamment sur :

- Les informations transmises par le service métier au service ID360 ;
- Les modalités proposées par le service ID360 en fonction des exigences du service métier ;
- La modalité choisie par l'Utilisateur et les autres informations qu'il communique au service ID360 ;
- La mise en œuvre de la vérification d'identité effectuée et les contrôles associés ;
- Les informations retournées par le service ID360 au service métier.

II.2.1. Contenu du dossier de preuve

Toutes les requêtes au service ID360 impliquent la constitution d'un dossier de preuve, contenant les éléments suivants :

- OID de politique applicable ;
- Trace horodatée de l'appel du service métier au service ID360 ;
- Numéro de requête affecté par le service ;
- Trace horodatée de la modalité choisie par l'Utilisateur et des informations associées ;
- Trace d'acceptation préalable de termes du service métier, et référence du document, le cas échéant ;
- Trace d'acceptation ou de refus des CGU le cas échéant ;
- Trace d'acceptation ou de refus du consentement à l'utilisation des données personnelles le cas échéant ;
- Trace des résultats de vérification d'identité fournis par la modalité utilisée ;
- Trace des événements relatifs à l'exécution des modalités propres du service ID360 ;
- Trace de validation du contrôle d'attribut de contact (OTP envoyé, OTP saisi, attribut de contact), le cas échéant,
- Résultat généré par le service ID360, hors images de titre, photo et documents collectés ;
- Référence de l'archive conservant le dossier de preuve.

Les modalités certifiées ou qualifiées conservent également des preuves conformément à leur pratique. Ces preuves peuvent être récupérées par le service métier pour compléter le dossier de preuves du service ID360.

Les données biométriques calculées à partir du visage de l'Utilisateur sont systématiquement supprimées une fois le résultat établi. Elles ne sont en aucun cas conservées ni, de fait, intégrées au dossier de preuve.

II.2.2. Conditions de conservation et d'accès du dossier de preuve

Le dossier de preuve est archivé dans un coffre-fort à valeur probatoire certifié NF461 pour une durée de 10 ans.

Au-delà du délai défini, les preuves sont détruites par le prestataire d'archivage à valeur probatoire.

Les dossiers de preuve sont accessibles en consultation :

- Directement par le service métier Via la console d'administration et par API;
- Par Docaposte dans le cas de droit d'accès aux données à caractère personnel que souhaite exercer un Utilisateur ;
- Par Docaposte pour la fourniture de preuves en cas de requête judiciaire ou en cas de suspicion de fraude,

Aucun autre traitement n'est appliqué aux dossiers de preuve.

Les accès sécurisés aux dossiers de preuves ne sont autorisés que pour les raisons indiquées ci-dessus et uniquement par :

- Les Utilisateurs habilités du service métier concerné,
- Les personnes habilitées Docaposte :
    - le responsable du service ID360,
    - administrateur système,

En complément, certaines modalités qualifiées ou certifiées conservent les éléments de preuve liés à leur service respectif pour une durée convenue lors de la phase de contractualisation entre cette modalité et le service métier, et sont au choix du service métier.

II.3. Obligations de Docaposte

Docaposte s'engage à :

- Fournir au service métier les Conditions Générales d'Utilisation liées au service ID360 pour intégration et dans ses propres conditions générales d'utilisation, et pour acceptation par les Utilisateurs finaux ;
- maintenir à jour et préserver l'intégrité des documents qu'elle publie ;
- assurer le contrôle de conformité de ses propres pratiques par rapport aux présents principes ;
- veiller à ce que l'ensemble des prestataires intervenant dans le service respectent les exigences de la présente politique ;
- être en mesure de répondre aux contrôles techniques et audits de qualité des procédures qui pourraient lui être demandés dans le cadre des obligations légales et de ses engagements ;
- contrôler à fréquence régulière les qualifications et certifications des modalités, et d'informer le service métier de l'échéance d'une perte de qualification ou certification.

II.4. Obligations du service métier

Un service métier doit :

- Soit contractualiser directement avec un ou plusieurs fournisseurs de modalité de vérification d'identité à distance, soit déléguer à Docaposte cette contractualisation ;
- S'enregistrer sur le service ID360, et protéger en intégrité et confidentialité les identifiants et secrets d'authentification qui lui sont remis à cette occasion ;
- Nommer des administrateurs responsables de la configuration du service ID360 et des Utilisateurs selon le rôle de chacun ;
- Adapter ses CGU à l'usage du service ID360, avec les mentions fournies par le prestataire Docaposte. Établir, conserver, présenter et faire accepter par l'Utilisateur ces Conditions Générales d'Utilisation;
- Reconnaître explicitement la valeur probatoire du dossier de preuve établi par le service ID360 ;
- Choisir les modalités offrant un niveau de garantie correspondant aux exigences liées à son usage ;
- Déclarer selon le process défini ci-après toute suspicion de fraude ou fraude avérée à Docaposte,
- Maintenir un haut niveau de sécurité de ses Systèmes d'informations,
- Conserver les éléments fournis par le service ID360 dans des conditions répondant aux exigences de sécurité et de confidentialité.

II.5. Obligations des Utilisateurs

L'Utilisateur doit :

- Accepter les Conditions Générales d'Utilisation du service métier, intégrant les conditions d'utilisation du service ID360 ;
- Accepter le cas échéant les Conditions Générales d'Utilisation de la modalité de vérification d'identité à distance qu'il utilise ;
- Reconnaître la valeur probatoire du dossier de preuve généré par le service ID360 ;
- Veiller à la protection des informations et des moyens qu'il utilise pour procéder à la vérification d'identité à distance ;
- Ne pas utiliser le service de façon illégale, en particulier ne pas tenter d'usurper l'identité d'un tiers ou présenter des informations erronées ou corrompues ;
- Informer sans délai Docaposte de toute usurpation ou tentative d'usurpation d'identité dont il aurait connaissance sur le service ID360.

II.6. Obligation des fournisseurs de modalités

Les fournisseurs de modalités doivent informer Docaposte des incidents de sécurité / perte de certification ou qualification.

II.7. Enregistrement et traitement des fraudes

Le processus d'enregistrement de suspicion d'usurpation d'identité, ou d'usurpation d'identité avérée est disponible :

- aux administrateurs des services métiers via l'adresse mail : sherlock.id@docaposte.fr;
- aux exploitants Docaposte.

L'email envoyé doit être chiffré en vue de la protection des données personnelles, et doit contenir les données suivantes de la part du réclamant :

- nom et prénom du demandeur;
- adresse e-mail du demandeur ;
- numéro de téléphone du demandeur ;
- description de l'usurpation d'identité suspectée ou avérée, avec référence du dossier concerné.

Ces alertes sont transmises :

- au responsable du service ID360 ;
- au référent à la protection des données Docaposte.

Quelle que soit l'origine de la demande, le responsable du service et/ou le référent à la protection des données initie une vérification en recueillant l'ensemble des éléments, y compris une copie du dossier de preuves.

Si la fraude est avérée, l'Utilisateur et le service métier concerné sont immédiatement prévenus. Le référent à la protection des données informe toute autorité de contrôle devant être informée.

Si la suspicion de fraude n'est pas avérée, le service métier est prévenu.

Le délai de traitement d'une déclaration de suspicion de fraude ou de fraude avérée ne peut excéder 72h.

La copie du dossier de preuves est systématiquement détruite.

II.8. Informations publiées concernant le service

Docaposte s'engage à publier au minimum les informations suivantes à destination des Utilisateurs du service et des tiers :

- Politique et pratiques du service (le présent document) ;
- Identification des documents complémentaires acceptés ;
- Conditions Générales d'Utilisation du service par les Utilisateurs finaux ;
- Politique de confidentialité des données.

Ces informations sont publiées en accès libre à l'adresse suivante :

https://www.id360docaposte.com/

Les informations sont publiées dès que nécessaire afin que soit assurée, à tout moment, leur cohérence avec les engagements, les moyens et les procédures en vigueur.

III. Gestion des risques

III.1. Analyse de risques

Avant l'ouverture du service, Docaposte effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, juridiques et commerciaux. Le service a ainsi fait l'objet :

- D'une analyse des risques métier ;
- D'une analyse des risques portant sur l'infrastructure.

Les mesures de sécurité nécessaires sont identifiées en tenant compte du résultat de ces études. Docaposte fixe en conséquence les exigences de sécurité et les procédures opérationnelles à mettre en œuvre sur le service. Celles-ci sont documentées dans le présent document et dans la politique de sécurité du système d'information.

Les analyses de risque sont réévaluées, et révisées si besoin, au moins tous les deux ans. Elles sont mises 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.

III.2. Analyse d'impact relative à la protection des données

Le service ID360 a fait l'objet d'une analyse d'impact relative à la protection des données à caractère personnel (AIPD) garantissant un traitement conforme au RGPD et respectueux de la vie privée.

III.3. Homologation de sécurité

La décision d'homologation de sécurité est prononcée par la direction de Docaposte sur la base des avis de différentes parties dont la DSI, le DPO et le service juridique. Elle atteste aux clients et Utilisateurs finaux du service que les risques qui pèsent sur eux, sur les informations traitées et sur les services rendus, sont minimes, connus et maîtrisés par Docaposte.

L'homologation est menée selon le process d'homologation interne de Docaposte, incluant l'acceptation des risques résiduels identifiés par les analyses de risque portant sur le service. Cette homologation est réalisée préalablement à l'ouverture du service puis révisée au moins tous les deux ans.

III.4. Politique de Sécurité du Système d'Information

Docaposte dispose d'une politique de sécurité du système d'information (PSSI) applicable au service. Cette PSSI est approuvée par la direction de Docaposte.

La PSSI, et ses versions successives, est accessible et transmise en premier lieu aux employés. Elle est également communiquée si nécessaire aux clients du service, aux prestataires et aux organismes d'évaluation.

Docaposte conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvre par des prestataires. En particulier, Docaposte s'assure de l'application des mesures prévues dans la PSSI par des audits de ces fonctions.

La PSSI exige la tenue d'un inventaire des actifs du SI. Cet inventaire est revu régulièrement et à chaque évolution de l'infrastructure. Tout changement susceptible d'avoir un impact sur le niveau de sécurité est soumis à l'approbation préalable du comité de pilotage du service.

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

IV. Gestion et exploitation du service

IV.1. Organisation interne

Docaposte dispose des moyens matériels, humains et financiers suffisants pour assurer l'exploitation du service conformément à cette politique.

Une organisation interne au sein de Docaposte est en place pour piloter et exécuter les processus définis pour la fourniture et la gestion du service. Les rôles sont définis de manière à séparer les responsabilités et à minimiser le risque d'action, intentionnelle ou non, portant atteinte à la sécurité des biens.

Les prestataires de Docaposte prenant part à la fourniture du service sont soumis à des obligations contractuelles permettant de garantir le niveau de sécurité global. En particulier, la présente politique et la PSSI leur sont transmises pour application. Docaposte s'assure que les prestations fournies par des tiers sont conformes aux attendus et qu'elles respectent les exigences fonctionnelles et de sécurité du service ID360. Docaposte conserve la responsabilité globale du respect des exigences de la présente politique.

Docaposte a souscrit une assurance de responsabilité civile professionnelle, couvrant ce service contre toutes les conséquences pécuniaires de sa responsabilité, résultant de dommages qui pourraient être causés aux clients et Utilisateurs du service.

IV.2. Ressources humaines

Les personnels de Docaposte et de ses prestataires sont les premiers acteurs de la sécurité et de la fiabilité des opérations du service. Docaposte s'assure donc du respect des exigences relatives aux ressources humaines, aussi bien en interne que chez ses prestataires.

IV.2.1. Compétences

Le personnel employé possède l'expertise, l'expérience et les qualifications nécessaires pour accomplir ses fonctions. Ce personnel est informé de la présente politique du service, de la PSSI applicable, des enjeux de sécurité du service et sensibilisé à la démarche éthique du groupe. Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité en vigueur. Ceci intègre en particulier les règles de sécurité relatives aux biens sensibles du SI et aux données à caractère personnel. Des sensibilisations régulières sont organisées, au minimum tous les ans, sur les nouvelles menaces et les bonnes pratiques de sécurité.

IV.2.2. Définition des rôles et responsabilité

Les rôles et responsabilités liés à la sécurité sont documentés dans des descriptions de poste. Docaposte respecte les principes de séparation des rôles et de moindre privilège dans la définition des fonctions et lors de leur affection. Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des règles de sécurité en vigueur au sein du service.

Des sanctions disciplinaires appropriées sont prévues pour les personnels dérogeant à la PSSI, à la politique ou aux pratiques du service.

IV.2.3. Définition des rôles de confiance

Les rôles de confiance, sur lesquels repose la sécurité du fonctionnement du service, sont clairement identifiés. Le personnel accédant à un rôle de confiance est nommé par la direction et accepte formellement cette fonction.

Les rôles de confiance définis sont :

- Responsable sécurité : Le responsable sécurité est le garant de la mise en œuvre de la politique de sécurité au niveau du service.
- Ingénieurs système : Les ingénieurs système sont les 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 l'infrastructure du service, ainsi que leur surveillance (supervision, détection d'incident).
- Opérateur : Les opérateurs sont les personnes en charge de processus métier non automatisés du service au sein de Docaposte, tels que la gestion des clients.
- Contrôleur : Personne autorisée à accéder aux preuves et archives du service.

Plusieurs rôles de confiance peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. A minima, le cumul des rôles de confiance suivants sont interdits :

- Ingénieur système et tout autre rôle ;
- Contrôleur et opérateur.

IV.2.4. Vérification des antécédents

Docaposte 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, et être libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations.

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

IV.3. Gestion des biens

IV.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.

IV.3.2. Supports

Les supports (papier, disque dur, bandes, CD, etc.) des biens sensibles sont gérés selon des procédures de sécurité adaptées à leur sensibilité.

Des mesures sont mises en œuvre afin de prévenir l'obsolescence, l'accès non autorisé, le vol ou l'altération des supports du service. Ces mesures sont effectives pour toute la durée de conservation prévue des biens.

En fin de vie, et selon des procédures en accord avec le niveau de confidentialité des informations qu'ils contiennent, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation.

IV.4. Contrôle d'accès

Docaposte met en œuvre un contrôle d'accès aux systèmes d'information du service.

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 est identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service. Les mesures de sécurité du contrôle d'accès garantissent le respect de la séparation des rôles, et en particulier l'accès aux

logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est strictement contrôlé. Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

Les informations sensibles sont protégées y compris contre une divulgation accidentelle qui résulterait de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.

La PSSI décrit en détail les règles de contrôle d'accès applicables au SI du service. Le contrôle d'accès au niveau réseau est décrit au §Sécurité opérationnelle.

IV.5. Cryptographie

Docaposte effectue une veille de sécurité concernant les moyens et mécanismes cryptographiques employés, pour garantir leur maintien à l'état de l'art et le traitement des vulnérabilités qui pourraient apparaître.

IV.6. Sécurité physique et environnementale

IV.6.1. Situation géographique et construction des sites

Les sites d'implantation des infrastructures du service ne sont pas soumis à des risques environnementaux naturels. Les autres risques naturels et technologiques sont pris en compte et traités.

La construction des sites respecte les règlements et normes en vigueur.

IV.6.2. Sécurité physique de l'infrastructure

Des mesures sont mises en œuvre afin de respecter les exigences et engagement de la présente politique en matière de disponibilité du service, en particulier concernant :

- L'alimentation électrique et climatisation ;
- La vulnérabilité aux dégâts des eaux ;
- Prévention et protection incendie

IV.6.3. Accès physique

L'accès aux composantes critiques du service est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux, et la traçabilité de ces 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, le vol ou l'altération des biens nécessaires au bon fonctionnement du service.

IV.6.4. Sauvegardes hors site

Des sauvegardes hors site sont effectuées au moins quotidiennement pour assurer la disponibilité des informations même en cas de sinistre majeur.

IV.7. Sécurité opérationnelle

IV.7.1. 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.

IV.7.1.a) 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 définie, notamment 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.

IV.7.1.b) 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.

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

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

Conformément au RGPD, Docaposte 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.

IV.7.2. Mesures liées à la gestion de la sécurité

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

IV.7.3. 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, l'analyse d'impact est effectuée dans les plus brefs délais suivant la publication de la vulnérabilité. Docaposte s'engage à traiter toute vulnérabilité critique dans un délai de 48 heures après sa découverte.

IV.7.4. 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.

IV.8. Sécurité réseau

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

- 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.
- L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les échanges nécessaires au fonctionnement de la composante au sein du SI du service. Le réseau interne du service est protégé des accès non autorisés, y compris de la part des clients ou partenaires du service. Des pares-feux sont configurés pour interdire tout accès ou protocole non strictement requis pour le fonctionnement du service.
- Docaposte 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.
- Tous les systèmes critiques sont isolés dans une ou plusieurs zones sécurisées.
- 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 sont pas utilisés à d'autres fins. Les systèmes de production du service sont séparés des systèmes utilisés pour le développement et les tests.
- La communication entre des systèmes de confiance distincts n'est établie qu'à travers des canaux sécurisés, logiquement ou physiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.
- Si un niveau élevé de disponibilité du service est nécessaire, la connexion réseau externe est redondante pour assurer la disponibilité des services.
- Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par Docaposte, est effectuée par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Cette analyse est réalisée a minima tous les trois mois et donne lieu à un rapport.
- Un test d'intrusion sur les systèmes du service est réalisé, lors de la mise en place, a minima tous les ans, et après toute évolution de l'infrastructure ou des applications, par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Ce test donne lieu à un rapport.

IV.9. 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.

Les activités de supervision sont menées en prenant en compte la sensibilité des informations collectées et analysées. A minima, les événements suivants sont supervisés :

- Le démarrage et l'arrêt des fonctions de journalisation ;
- La disponibilité et l'utilisation des services requis via le réseau du service.

Docaposte a mis en place une organisation capable de réagir 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 visent à minimiser les dommages causés par les incidents de sécurité et les dysfonctionnements.

Par ailleurs, Docaposte mesure en continu le taux de disponibilité du service et la charge constatée afin de s'assurer de l'adéquation des moyens mis en œuvre vis-à-vis des engagements contractuels avec ses clients et des obligations de cette politique.

IV.9.1. Procédures de remontée et de traitement des incidents et des compromissions

Docaposte notifie toute autorité compétente dans un délai maximal de 24 heures après en avoir eu connaissance, toute atteinte à la sécurité des 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, Docaposte informe sans délai la personne physique ou morale concernée.

IV.10. Gestion des traces

IV.10.1. 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 journalise au minimum 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 suite à 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 sont aussi 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
- Les actions de maintenance et de changements de la configuration des systèmes
- Les changements apportés au personnel
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les Utilisateurs…).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions du service, des événements spécifiques aux différentes fonctions du service sont également journalisés, notamment :

- Vérification d'identité d'un Utilisateur ;
- Gestion des clients du service ;
- Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) ;
- Paramétrage du service par un administrateur client ;
- Gestion des modalités du service par un administrateur Docaposte.

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 se fait, sauf exception, le même jour ouvré que l'événement. Les événements et données spécifiques à journaliser sont documentés par Docaposte.

IV.10.2. 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 effectué périodiquement afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

IV.10.3. Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins un mois. Ils sont archivés le plus rapidement possible et au plus tard quinze jours après leur génération.

IV.10.4. 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 précision de l'horloge données dans cette 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.

IV.10.5. 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.

IV.11. Archivage des données

IV.11.1. Types de données à archiver

Docaposte conserve pendant une durée minimale de 10 (dix) ans après la réalisation d'une vérification d'identité, toutes les informations pertinentes concernant les données reçue et délivrées, notamment afin de pouvoir fournir des preuves en justice.

Les données à conserver sont au moins :

- les dossiers de preuve ;
- les versions successives des documents publiés (politique et pratiques du service, CGU, ...) ;
- les rapports d'audit.

IV.11.2. Période de conservation des archives

La durée de conservation, les modalités de réversibilité et de portabilité sont précisées dans les conditions générales d'utilisation du service.

Les journaux d'événements sont archivés pendant dix ans après leur génération.

IV.11.3. Protection des archives

Les moyens mis en œuvre pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

Pendant tout le temps de leur conservation, les archives sont :

- protégées en intégrité ;
- accessibles aux seules personnes autorisées ;
- formatées pour pouvoir être relues et exploitées.

IV.11.4. Exigences d'horodatage des données

Les événements liés à l'archivage des données sont horodatés conformément aux exigences données dans cette politique.

IV.11.5. Procédures de récupération et de vérification des archives

Seul Docaposte a accès aux archives.

IV.12.Continuité d'activité

IV.12.1. Reprise suite à la compromission et sinistre

Docaposte a défini et maintient un plan de continuité d'activité du service pour réagir à un incident majeur. Ce plan est testé annuellement.

Chaque entité opérant une 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.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques (p. ex., clés privées ou données à caractère personnel), Docaposte en est immédiatement informé et le traite dans la plus grande urgence, voire immédiatement. Lorsqu'ils sont impactés, les clients, Utilisateurs et partenaires du service en sont informés sans délai par tout moyen utile et disponible (presse, site Internet, récépissé...). Le service est rétabli, après résolution de l'incident, dans les délais définis par le plan de continuité d'activité du service.

Si l'une des modalités de vérification d'identité subit un incident majeur (indisponibilité, compromission, vulnérabilité, obsolescence de moyens cryptographiques...), alors Docaposte :

- interrompt toute utilisation de cette modalité jusqu'à la fin du traitement de l'incident ;
- informe tous les clients, Utilisateurs et tiers impactés.

IV.13.Fin d'activité

Docaposte a établi un plan de cessation d'activité du service dans le but de minimiser les impacts sur les parties prenantes, et en particulier de leur garantir la possibilité de bénéficier des preuves associées au service rendu.

Le plan de cessation d'activité du service prévoit :

- L'information préalable, avec un préavis d'au minimum trois (3) mois, des différentes parties suivantes : clients, fournisseurs des modalités de vérification d'identité et organisme d'audit du service.
- La date de fin d'activité du service est communiquée, avec un préavis d'au minimum un mois, sur le site du service pour information de toutes les autres parties intéressées ;
- La terminaison des contrats passés avec d'autres entités pour la réalisation des vérifications d'identité à distance, en particulier avec les fournisseurs des modalités de vérification d'identité ;
- L'archivage, pour la durée nominale restant à couvrir, de toutes les preuves générées par le service jusqu'à sa cessation d'activité ;
- La destruction de toutes les clés cryptographiques privées et secrètes, y compris de leurs copies, utilisées par le service pour le fonctionnement ou la production de nouvelles preuves du service ;
- La recherche de solutions alternatives du marché pour les clients du service, et le cas échéant, la recherche d'accords pour le transfert de l'activité.

Docaposte a provisionné les moyens financiers nécessaires à la gestion de la fin d'activité du service.

IV.14. Conformité

Les pratiques de Docaposte sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de Docaposte 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 »[1]. Une étude éthique, encadrant les usages d'intelligence artificielle et intégrant la sensibilisation des personnels est menée. Cette étude éthique fait partie intégrante de l'avis d'homologation du service.

Docaposte garantit la conformité avec les exigences légales et règlementaires. Le respect des exigences légales, et en particulier la protection des données personnelles est présentée dans un chapitre dédié.

[1] https://www.w3.org/Translations/WCAG20-fr/

V. Autres problématiques métiers et légales

V.1. Responsabilité financière

Docaposte 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.

V.1.1. Couverture par les assurances

Docaposte atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrite dans ce document, ainsi qu'une assurance sur les risques Cyber.

V.1.2. Couverture et garantie concernant les entités utilisatrices

La couverture et les garanties concernant les entités utilisatrices sont exposées dans les Conditions Générales d'Utilisation du service.

V.2. Confidentialité des données personnelles

V.2.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des Utilisateurs et les justificatifs associés ;
- Les causes de révocations des moyens d'authentification ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, etc.).

V.2.2. Responsabilités en termes de protection des informations confidentielles

Docaposte respecte la législation et la réglementation en vigueur sur le territoire français et est responsable de la protection des informations confidentielles.

Docaposte peut cependant devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Les clients peuvent également accéder à leurs données professionnelles auprès de Docaposte.

V.3. Protection des données personnelles

V.3.1. Politique de protection des données personnelles

Les Utilisateurs du service ID360 sont informés que, dans le cadre du service, Docaposte est amenée à collecter, héberger, et traiter des données à caractère personnel les concernant, aux seules fins d'assurer la vérification d'identité. Docaposte veillant notamment, dès la conception de son service, à limiter la quantité de données traitée dès le départ (principe dit de minimisation).

Docaposte s'engage à conserver confidentielles les données personnelles des Utilisateurs et à ne pas les divulguer à des tiers, pendant toute la durée de leur conservation. Pour ce faire, Docaposte fera ses meilleurs efforts pour :

- Prendre toutes les précautions utiles et mettre en place des contrôles efficaces de protection afin de préserver la sécurité des Données Personnelles, et notamment empêcher qu'elles ne soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;
- Disposer des moyens organisationnels, techniques et financiers permettant de garantir la mise en œuvre des mesures de confidentialité et de sécurité ;

- Prendre toute mesure de sécurité pour assurer la conservation et l'intégrité des données

V.3.2. Informations à caractère personnel

Les informations considérées comme des données à caractère personnel sont au minimum les suivantes :

- Les données d'identité des Utilisateurs ;
- Les documents complémentaires contrôlés ;
- Les traces relatives aux vérifications d'identité réalisées par les Utilisateurs (service métier sollicité, identité de l'Utilisateur, datation, modalités de vérification utilisée, ...) ainsi que les informations techniques collectées (adresses IP, navigateurs...) à cette occasion.

Le service ID360 ne conserve aucune donnée biométrique. Les gabarits calculés sur les visages sont supprimés directement après traitement de comparaison faciale et ne sont ni transmis ni conservés.

Conformément à la règlementation, les Utilisateurs disposent d'un accès en consultation à leurs données à caractère personnel conservées par le service jusqu'à la fin de leur période d'archivage. Toutefois, du fait de leur statut de preuve, la rectification ou la suppression des données à caractère personnel contenues dans les journaux d'événements et les archives du service ne sont pas autorisées. Les durées et finalité de conservation de ces données sont précisées dans les chapitres relatifs à la gestion des traces et à l'archivage des données.

V.3.3. Responsabilité en termes de protection des données personnelles

Docaposte s'engage à respecter la réglementation légale applicable au traitement de données personnelles et notamment le respect du règlement général de protection des données [RGPD].

Responsable de traitement

Dans le cadre de la fourniture du service ID 360 appartenant à Docaposte, l'entreprise utilisatrice du service est, au sens de l'article 4 paragraphe 7 du RGPD, réputée responsable de traitement.

Sous-traitant

Docaposte agit en tant que sous-traitant du responsable de traitement.

V.3.4. Notification et consentement d'utilisation des données personnelles

Les Utilisateurs sont informés des conditions d'utilisation de leurs données personnelles dans les Conditions Générales d'Utilisation du service de l'entreprise utilisatrice, qu'ils doivent lire et accepter avant de bénéficier du service ID360, ainsi que dans la politique de confidentialité du service ID360.

V.3.5. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Docaposte se conforme strictement aux dispositions légales pour traiter les demandes de divulgation d'informations personnelles aux autorités judiciaires ou administratives.

V.3.6. Autres circonstances de divulgation d'informations personnelles

Docaposte n'a pas prévu d'autres circonstances de divulgation d'informations personnelles.

V.4. Droit sur la propriété intellectuelle et industrielle

Docaposte est titulaire de l'intégralité des droits de propriété intellectuelle et/ou matérielle sur le service ID360, les progiciels, logiciels, développements, paramétrages, méthodes, savoir-faire, outils de développement, fichiers, bases de données, données, documents, en ce compris le contenu du site, les signes distinctifs, dessins, modèles, matériels (ci-après dénommés ensemble « les Éléments»), qui sont sa propriété et qui sont utilisés ou rendus accessibles aux Utilisateurs dans le cadre du service ID360.

Aucun transfert des droits de propriété intellectuelle et/ou matérielle n'est opéré sur les Éléments dont Docaposte est propriétaire ou pour lesquels Docaposte a obtenu une licence ou un droit d'usage et qui sont utilisés ou rendus accessibles aux Utilisateurs. Réciproquement, aucun transfert des droits de propriété intellectuelle et/ou matérielle n'est opéré sur les Éléments dont l'Utilisateur est propriétaire et qui sont utilisés ou rendus accessibles à Docaposte.

Docaposte concède à l'Utilisateur un droit d'utilisation personnel incessible et non exclusif. Cette licence est consentie pendant toute la durée du Contrat uniquement et ce, aux seules fins d'utilisation de la Solution pendant cette même période.

V.5. Interprétations contractuelles et garanties

Les intitulés des articles, paragraphes, annexes et table des matières ne sont donnés qu'à titre de référence et de commodité. Ils ne font pas partie intégrante, ni n'entrent dans l'interprétation de la présente Politique.

V.6. Juridictions compétentes

La présente politique est soumise au droit français.

V.7. Dispositions concernant la résolution de conflits

En cas de litige sur l'interprétation ou l'exécution de la présente politique, pour le cas où les parties ne parviendraient pas à trouver un accord amiable dans un délai de 30 jours sauf à ce que ce délai soit reconduit expressément entre les parties, il est attribué compétence expresse et exclusive au tribunal de commerce de Paris, lequel sera la seule juridiction compétente pour connaitre de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou les oppositions sur injonction de payer.

V.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.