Service de Garantie de l'Identité Numérique

Analyse d'impact relative à la protection des données

Mention préalable

Le présent document constitue une version communicable de l'analyse d'impact relative à la protection des données du Service de Garantie de l'Identité Numérique.

Certaines informations ont fait l'objet d'occultations préalables à sa communication, conformément aux dispositions de l'article L311-5 du Code des relations entre le public et l'administration, dès lors que leur divulgation serait susceptible de porter atteinte *« à la sûreté de l'État, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations »*.

Sommaire

Glossaire

Données d'identité	Données d'identification issues du composant électronique de la CNIe. Ces informations comprennent le nom, le nom d'usage, le(s) prénom(s), la date de naissance, le lieu de naissance, l'adresse postale, la nationalité et le sexe.
France Identité	Application mobile permettant à l'usager d'activer et d'utiliser le moyen d'identification électronique SGIN, notamment pour s'authentifier auprès de services en ligne et générer des attestations.
Identification électronique	Processus consistant à utiliser des données d'identification personnelle sous une forme électronique afin d'identifier de manière unique une personne physique.
Authentification	Processus électronique permettant de confirmer l'identification électronique d'une personne physique, ou de confirmer l'origine et l'intégrité de données sous forme électronique.
Moyen d'identification électronique	Ensemble d'éléments matériels ou immatériels, utilisés pour l'identification électronique d'une personne physique, comprenant des données d'identification personnelle et, le cas échéant, des dispositifs ou informations d'authentification.
Usager	Personne physique majeure, titulaire d'une carte nationale d'identité électronique (CNIe) délivrée par l'État français, qui a activé son Moyen d'Identification Électronique (MIE) via l'application mobile France Identité.
Interopérabilité	Capacité de systèmes d'identification électronique et de services de confiance à fonctionner de manière cohérente entre États membres, permettant une utilisation transfrontière.

1. Étude du contexte

1.1. Vue d'ensemble

1.1.1. *Présentation du traitement*

L'avènement d'une identité numérique sécurisée

La numérisation croissante des interactions entre les citoyens, les entreprises et les administrations a profondément transformé les usages et les attentes en matière d'identification d'une personne physique à un service.

Aujourd'hui, la quasi-totalité des services en ligne requiert une preuve préalable d'identité, qu'il s'agisse d'accéder à des services publics, de réaliser des paiements sécurisés ou encore de prouver son âge pour certaines démarches. L'essor du numérique a ainsi fait émerger un besoin de solutions d'identification électronique fiables, capables de garantir à la fois la sécurité des transactions et la protection des données personnelles.

Toutefois, cette transition s'est accompagnée d'un nouveau risque, la fraude à l'identité, devenue l'un des principaux vecteurs de cybercriminalité. L'usurpation d'identité en ligne a explosé ces dernières années, facilitée par la multiplication des comptes numériques, la circulation massive de données personnelles sur Internet et l'interconnexion croissante des bases de données. Les fraudeurs exploitent ces vulnérabilités pour accéder à des services en se faisant passer pour d'autres utilisateurs, falsifier des documents électroniques ou détourner des identités à des fins financières et administratives.

De surcroît, chaque service en ligne impose ses propres règles d'authentification, souvent fondées sur des mots de passe, adresses emails ou des SMS, insuffisants face aux techniques de fraude de plus en plus sophistiquées (phishing, vol de sessions, falsification de justificatifs d'identité). Cette fragmentation de solutions, parfois peu sécurisées a accentué le manque de confiance des citoyens dans l'identité numérique. Certains se retrouvent contraints de multiplier les identifiants et les justificatifs demandés, augmentant ainsi les risques de compromission, tandis que d'autres sont exclus des services numériques faute de solutions adaptées et accessibles. Cette situation met en lumière le besoin d'une solution d'identification unifiée, sécurisée et reconnue à l'échelle nationale et européenne.

Cette disparité des solutions d'authentification en ligne et l'absence de reconnaissance mutuelle entre États membres ont révélé la nécessité d'édicter un cadre harmonisé, garantissant aux citoyens à la fois la fiabilité, la protection des données et l'accessibilité aux services numériques. Pour répondre à cet impératif, la dématérialisation des titres d'identité s'est imposée comme une solution essentielle afin d'assurer l'authenticité de l'identité d'un ressortissant et unifier les standards de sécurité.

L'Union européenne a ainsi développé un cadre réglementaire structuré, visant à instaurer une identité numérique souveraine, sécurisée et reconnue entre les Etats membres.

Un cadre juridique européen unifié

C'est dans cette perspective que le règlement eIDAS (UE 910/2014)[1] a instauré un cadre unifié pour l'identification électronique et les services de confiance au sein du marché intérieur. Ce règlement a pour objectif d'harmoniser les moyens d'identification électronique et garantir leur reconnaissance mutuelle entre États membres. Ce cadre s'applique également aux identités régaliennes, fondées sur l'état civil des citoyens et attestées par des titres d'identité officiels, tels que la Carte Nationale d'Identité Électronique (CNIe) en France. En permettant à un usager d'utiliser un moyen d'identification électronique souverain et reconnu à l'échelle européenne, eIDAS a facilité l'accès aux services publics et privés en ligne, y compris lorsqu'ils sont situés dans un autre État membre.

L'identification électronique repose sur un moyen d'identification électronique (MIE), défini comme un élément matériel ou immatériel permettant à une personne de prouver son identité pour accéder à un service numérique. Ce dispositif peut prendre différentes formes, notamment un titre d'identité électronique intégrant une puce sécurisée contenant des données d'identité, ou encore un système d'authentification numérique accessible via une application mobile, générant des preuves d'identité conformes aux exigences réglementaires.

Présentation du traitement Service de Garantie de l'Identité Numérique (SGIN)

[1] Règlement (UE) No 910/2014 du 23 juillet 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

En France, la sécurisation de l'identité numérique s'est concrétisée par la mise en place du Service de Garantie de l'Identité Numérique (SGIN), instauré par le décret n° 2022-676 du 26 avril 2022[2].

Ce traitement de données à caractère personnel, également désigné par l'acronyme « *SGIN* », constitue un moyen d'identification électronique (MIE) permettant aux citoyens français titulaires d'une Carte Nationale d'Identité Électronique (CNIe) de s'authentifier à des téléservices d'organismes publics ou privés. Le SGIN permet également la génération d'attestations électroniques d'identité, offrant aux citoyens la possibilité de créer des justificatifs d'identité à usage unique, utilisables à la place d'une photocopie de pièce d'identité pour différentes démarches administratives ou commerciales.

Ce dispositif, mis en œuvre par le ministère de l'Intérieur et l'Agence Nationale des Titres Sécurisés (ANTS), repose sur une application mobile dédiée, France Identité, installée volontairement par l'usager sur son smartphone. Cette application permet de lire sans contact, via la technologie NFC, la puce électronique intégrée à la CNIe et d'utiliser les données d'identité qu'elle contient afin de produire une preuve d'identification numérique.

Le composant électronique de la CNIe, lu par l'application mobile France Identité, contient les attributs d'identité essentiels de l'usager, notamment ses nom et le nom d'usage le cas échéant, prénoms, date et lieu de naissance, sexe et nationalité, ainsi que les références du titre d'identité, incluant son numéro, sa date de délivrance et sa date de fin de validité.

Le Service de Garantie de l'Identité Numérique a été conçu pour répondre aux risques précités. Il vise à simplifier les démarches administratives, en permettant aux citoyens d'éviter la transmission de copies physiques de leurs pièces d'identité lors de l'accès à un service en ligne. Il contribue également à renforcer la sécurité des échanges numériques, en limitant les risques d'usurpation d'identité grâce à une vérification fiable des données issues du titre d'identité. Enfin, en facilitant l'authentification des usagers auprès de services publics et privés, le SGIN favorise le développement d'une identité numérique régalienne, interopérable et conforme aux standards européens.

Evolution du traitement et conformité au RGPD

Le 28 août 2021, le SGIN a fait l'objet d'une première analyse d'impact relative à la protection des données (AIPD), à l'issue de laquelle le responsable de traitement avait estimé que « *le niveau des risques résiduels* » était maîtrisé. Le traitement a également

[2] Décret n° 2022-676 du 26 avril 2022 autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN).

reçu deux avis favorables de la CNIL[3] , qui ont salué les garanties mises en place en matière de sécurité, de minimisation des données et de maîtrise par l'usager de son identité numérique.

Depuis, le traitement s'est inscrit dans un cadre juridique renforcé, avec la publication du décret SGIN, le 26 avril 2022 et l'obtention de la certification de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[4] pour un niveau de garantie *« élevé »*, conformément aux exigences de l'article 8 du règlement eIDAS. Cette certification est indispensable pour assurer la reconnaissance mutuelle des moyens d'identification électronique au sein de l'Union européenne et garantir l'interopérabilité du SGIN avec les infrastructures numériques des autres États membres.

Par ailleurs, l'entrée en vigueur du règlement eIDAS 2 (UE 2024/1183)[5] marque une nouvelle étape dans le développement de l'identité numérique régalienne en Europe. Cette révision introduit le Portefeuille d'Identité Numérique Européen (EUDI Wallet) et renforce les exigences en matière d'interopérabilité, d'attributs qualifiés et de contrôle par l'usager. Dans ce contexte, l'adaptation du SGIN aux nouveaux usages liés à la présentation d'attributs d'identité, y compris en proximité, nécessite la mise à jour de l'AIPD initiale.

La présente analyse vise par conséquent, à réévaluer les risques et les mesures de protection associées, en tenant compte à la fois des évolutions techniques du système et des nouvelles exigences issues d'eIDAS 2. Elle a vocation à garantir la conformité stricte du traitement au cadre juridique national et européen, tout en renforçant la confiance dans l'usage d'une identité numérique sécurisée, maîtrisée par l'usager et pleinement intégrée dans l'écosystème numérique européen.

[3] Délibération n° 2021-151 du 9 décembre 2021 portant avis sur un projet de décret en Conseil d'Etat autorisant la création d'un moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » et Délibération n° 2022-011 du 10 février 2022

[4] Certification ANSSI § n° 244 du 7 février 2024

[5] Règlement (UE) 2024/1183 du 11 avril 2024 modifiant le règlement (UE) no 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique

Description du traitement	**Enrôlement :** L'usager active son identité numérique en lisant sa CNIe via l'application France Identité. Les données nécessaires sont alors utilisées pour créer une identité numérique sur son terminal. Les données d'identité sont conservées sous le contrôle exclusif de l'usager.
	Authentification à des services en ligne : L'usager peut prouver son identité pour accéder à des services connectés via FranceConnect ou directement raccordés au SGIN.
	Génération d'attestations d'identité : L'usager peut générer, depuis l'application, une attestation d'identité contenant uniquement les informations nécessaires. Cette attestation est produite dans des conditions garantissant son authenticité et la protection des données personnelles.
	Présentation en proximité : Une attestation d'identité simplifiée peut être affichée dans l'application sous forme de carte numérique. Elle peut être présentée pour vérification dans des situations nécessitant un contrôle rapide de l'identité, sans divulgation de données excessives.
Finalités du traitement	**Fournir aux usagers un moyen d'identification électronique régalien,** fondé sur la carte nationale d'identité électronique, leur permettant de s'authentifier auprès de services publics ou privés en ligne ou en proximité. **Permettre la génération, à l'initiative de l'usager, d'une attestation électronique d'identité,** signée par l'État, destinée à justifier ponctuellement de son identité auprès d'un tiers, sans présenter physiquement son titre d'identité.

	Garantir l'intégrité, la validité et la sécurité des titres et données d'identité traités, par l'usage de signatures électroniques et de QR codes sécurisés. **Faciliter la présentation d'une identité certifiée dans des situations de contrôle en proximité**, à l'aide d'un QR code dynamique
Enjeux du traitement	**Enjeu de sécurité et d'intégrité de l'identité numérique** Le traitement repose sur la transmission sécurisée des données d'identité certifiées, extraites du composant électronique sécurisé de la CNIe. Toute compromission ou altération pourrait permettre une usurpation d'identité ou une utilisation frauduleuse d'une fausse identité numérique. **Enjeu de minimisation et de limitation des données** Le SGIN doit garantir que seules les données strictement nécessaires à la finalité poursuivie sont traitées, tant dans les parcours d'authentification que dans la génération d'attestations. La capacité à générer des attestations à contenu restreint ou à usage unique (avec finalité) est essentielle pour éviter la collecte inutile des données et le risque de réutilisation abusive. **Enjeu de maîtrise par l'usager et de transparence** Le traitement garantit que l'usager conserve la maîtrise de ses données (génération à son initiative, conservation locale, aucune conservation par l'État). Il s'accompagne d'une information claire, notamment sur les modalités de vérification, de durée de validité, et d'opposabilité de l'attestation.
Responsable du traitement	La **collecte**, la **conservation** et le **traitement des informations** sont sous la responsabilité conjointe du Secrétariat général du ministère de l'Intérieur (SGMI) et de l'Agence Nationale des Titres Sécurisés (ANTS).

Sous-traitant(s)	Le traitement s'appuie sur des prestataires techniques intervenant notamment pour l'hébergement, la maintenance, le support et le développement du système d'information. Ces prestataires sont soumis à des obligations contractuelles strictes en matière de sécurité, de confidentialité et de protection des données à caractère personnel, conformément à l'article 28 du règlement général sur la protection des données.

1.1.2. *Les responsabilités liées au traitement*

L'Agence Nationale des Titres Sécurisés (ANTS) et le Secrétariat général du ministère de l'Intérieur (SGMI) sont conjointement responsables du traitement des données à caractère personnel mises en œuvre dans le cadre du SGIN. Plus précisément, l'ANTS traite les données d'identité extraites de la puce de la CNIe, dans le cadre de l'activation et de l'utilisation du moyen d'identification électronique par l'usager.

L'information des usagers est assurée par l'affichage, au moment de l'activation, d'une fenêtre modale précisant les conditions de traitement de leurs données personnelles, ainsi que par un lien vers la politique de protection des données du SGIN. Cf : Détermination et description des mesures pour l'information des personnes.

1.1.3. *Recensement des référentiels applicables au traitement*

Textes applicables au traitement	Modalités
La loi n°2012-410 du 27 mars 2012 relative à la protection de l'identité. Elle définit les données contenues dans le composant électronique de la carte d'identité et dispose que l'identité du possesseur de cette carte est justifiée à partir des données inscrites sur le document lui-même ou dans le composant électronique sécurisé.	***Oui***
La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. Elle établit des principes de base concernant la collecte, le stockage et l'utilisation des données personnelles.	***Oui***
L'article L. 102 du Code des postes et des communications électroniques. Il traite spécifiquement des moyens d'identification électronique, prévoyant qu'ils peuvent être certifiés par l'État, et crée	***Oui***

une présomption simple de fiabilité pour ceux-ci au sens de l'article 1354 du code civil.	
Le Code des relations entre le public et l'administration, notamment ses articles L. 112-9, L. 113-12 et L. 114-8	***Oui***
Le décret SGIN n° 2022-676 du 26 avril 2022. Il autorise la création du moyen d'identification électronique dénommé « Service de garantie de l'identité numérique » (SGIN).	***Oui***
L'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les utilisateurs et les autorités administratives et entre les autorités administratives	***Oui***
L'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité (RGS). Il établit un cadre normatif contraignant destiné à assurer la sécurité des systèmes d'information utilisés par les administrations françaises, afin de renforcer la confiance des usagers dans ces services. Il aborde différents aspects de la sécurité informatique, y compris les procédures de validation des certificats électroniques	***Oui***
L'arrêté du 20 septembre 2019 portant référentiel général d'amélioration de l'accessibilité (RGAA). Il définit les normes d'accessibilité applicables aux services en ligne.	***Oui***
Textes internationaux (collecte de données)	
Le règlement eIDAS 2, (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024, relatif à l'établissement du cadre européen relatif à une identité numérique, modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique ;	***Oui***
Règlement Général sur la Protection des données (RGPD), (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)	***Oui***
Le règlement relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union (UE) 2025/1208 du 12 juin 2025, renforce les normes de sécurité applicables aux cartes d'identité des citoyens de l'Union, il impose notamment aux États membres d'intégrer dans la carte nationale d'identité un composant électronique contenant des données biométriques (image faciale et empreintes digitales), dans un support de stockage hautement sécurisé. À défaut, les cartes non conformes cesseront d'être valables, au plus tard, le 3 août 2031.	***Oui***

1.1.4. *Les données traitées*

Les données traitées dans le SGIN se répartissent en plusieurs catégories :

Catégorie de données	Détails
Données d'identification issues du titre	• Nom • Prénoms • Nom d'usage • Sexe • Date de naissance • Libellé du lieu naissance • Nationalité • Numéro du titre
Données de l'attestation d'attributs d'identité	• Attributs sélectionnés parmi ceux ci-dessus • Finalité déclarée par l'usager (facultative) • Date de génération • Durée de validité • QR code signé • Identifiant technique de l'attestation (non personnel)
Autres données	• Données techniques nécessaires au fonctionnement et à la sécurité du service, notamment des données de connexion et de journalisation, conservées pour des durées limitées

1.1.5. Description fonctionnelle du processus

1.1.6. ***Enrôlement de l'identité numérique***

Le traitement SGIN et son application mobile France Identité, permet à tout citoyen français détenteur d'une carte nationale d'identité électronique de créer une identité numérique hautement sécurisée. Ce moyen d'identification électronique régalien conforme au niveau de garantie *« élevé »* du règlement eIDAS, vise à lutter contre l'usurpation d'identité en garantissant l'identité des usagers en ligne.

Le processus ci-dessous, décrit les étapes successives de l'activation du MIE par la personne concernée, de la préparation technique jusqu'à la création effective de son identité numérique.

Prérequis et éligibilité à l'utilisation de France Identité

> Âge et titre d'identité : être majeur et titulaire d'une carte d'identité nationale électronique en cours de validité ;

> Smartphone compatible : disposer d'un smartphone équipé de la technologie sans contact (NFC) et d'une version du système d'exploitation permettant de garantir un niveau de sécurité adapté au traitement des données d'identité. Le terminal doit notamment intégrer des mécanismes de protection assurant le stockage sécurisé de ces données.

Une fois ces deux prérequis réunis, le parcours d'enrôlement peut alors débuter sur l'application France Identité. L'usager doit avoir installé l'application mobile disponible dans les stores officiels et accepter les conditions générales d'utilisation lors de la création de son compte. L'usager définit un code personnel ou utilise le mécanisme de déverrouillage du terminal pour protéger l'accès à l'identité numérique.

La procédure d'enrôlement se déroule en 4 étapes successives :

(1) La lecture de la carte d'identité

Le processus d'enrôlement débute lorsque l'usager ouvre l'application France Identité et lance la procédure d'activation de son identité numérique.

Afin d'autoriser la lecture de son titre, l'usager saisit un code figurant sur sa carte nationale d'identité électronique. Il procède ensuite à une lecture sans contact de son titre à l'aide de son smartphone.

L'application lit alors les données nécessaires à l'activation de l'identité numérique. Des contrôles automatisés sont réalisés afin de vérifier l'authenticité du titre et l'intégrité des données.

En cas d'échec de la lecture ou des vérifications, la procédure d'enrôlement est interrompue.

(2) La vérification de la validité du titre physique

Une fois les données lues dans la puce du titre via la technologie sans contact (NFC), des vérifications à distance sont réalisées afin de s'assurer que le titre présenté par l'usager est valide. Cette étape vise à garantir que seul un titre d'identité en cours de validité peut servir de fondement à la création d'une identité numérique régalienne.

Des vérifications automatisées sont mises en œuvre afin de confirmer la validité du titre présenté, dans des conditions garantissant la sécurité et la confidentialité des données. Les données utilisées sont strictement limitées à ce qui est nécessaire à cette opération.

À l'issue de ces vérifications, lorsque le titre est confirmé comme valide, le parcours d'enrôlement peut se poursuivre. À l'inverse, si le titre ne peut être confirmé ou si une anomalie est détectée, la procédure est interrompue afin de prévenir tout risque d'utilisation frauduleuse.

Des contrôles complémentaires sont également mis en œuvre afin de vérifier que le moyen d'identification électronique associé au titre est actif et peut être utilisé conformément aux exigences de sécurité applicables. En cas d'invalidation du titre, y compris postérieurement à l'enrôlement, l'identité numérique associée peut être désactivée.

Cette étape constitue une garantie essentielle permettant de s'assurer que le titre utilisé est administrativement valide au moment de l'enrôlement, condition préalable à la délivrance d'un moyen d'identification électronique conforme aux standards de sécurité européens.

(3) La vérification de l'identité de l'usager

Une fois le titre lu et sa validité confirmée, le système vérifie que la personne procédant à l'enrôlement est bien son titulaire. À cette fin, deux modalités de vérification sont proposées à l'usager.

Vérification numérique via FranceConnect

L'usager peut choisir de confirmer son identité en s'authentifiant via FranceConnect, le dispositif d'identification proposé par l'État permettant d'accéder de manière sécurisée à de nombreux services en ligne.

Cette vérification repose sur la comparaison automatisée de données d'identité issues de sources reconnues comme fiables, notamment celles extraites du titre d'identité électronique et celles fournies par le fournisseur d'identité utilisé dans le cadre de FranceConnect. Ces sources s'appuient sur des référentiels faisant autorité en matière d'état civil.

Les données mobilisées pour cette opération sont strictement limitées à ce qui est nécessaire à la vérification, traitées uniquement pendant la durée requise et ne sont pas conservées à l'issue du rapprochement.

Vérification par voie postale

À défaut, l'usager peut recourir à une procédure de vérification reposant sur l'envoi d'un courrier sécurisé à son domicile. Cette modalité comporte plusieurs contrôles destinés à s'assurer que seule la personne titulaire du titre peut activer l'identité numérique.

Après confirmation de ses coordonnées, un code d'activation est adressé à l'usager selon un procédé garantissant un niveau approprié de sécurité. L'activation de ce code, associée à des vérifications complémentaires, permet de confirmer l'identité de l'usager et la cohérence des informations fournies.

Lorsque les vérifications sont concluantes, l'usager peut poursuivre le parcours d'enrôlement. Dans le cas contraire, la procédure est interrompue afin de prévenir tout risque d'usurpation d'identité. En cas de difficulté, des mécanismes permettent à l'usager de renouveler la démarche ou de corriger les informations nécessaires.

Ces modalités contribuent à garantir un niveau de confiance élevé dans la délivrance du moyen d'identification électronique.

(4) La finalisation du parcours d'enrôlement

Pour finaliser l'enrôlement, l'application France Identité invite l'usager à définir un « code personnel » (ci-après désigné, « code PIN » pour '*Personal Identification Number*' dans la présente analyse) propre à son moyen d'identification électronique, lui permettant d'utiliser son identité numérique en toute sécurité. La définition de ce code PIN est suivie d'une lecture de la CNIe via NFC afin de l'inscrire dans la puce du titre. À ce stade, le code choisi par l'usager est donc clairement distinct de celui de son smartphone.

Par ailleurs, l'application France Identité offre à l'usager, dans certains cas, l'option de remplacer son code PIN par le mécanisme de déverrouillage de son smartphone, géré par le système d'exploitation (iOS ou Android) et préalablement configuré dans les paramètres du téléphone selon ses préférences. Ce mécanisme peut reposer sur une authentification biométrique (reconnaissance faciale, empreinte digitale) ou sur le code de déverrouillage de l'appareil, utilisé ici comme facteur local d'authentification.

Si l'usager choisit cette option, il n'est plus invité par une interface France Identité à saisir son code PIN, mais par la fenêtre habituelle de son système d'exploitation, comme lorsqu'il déverrouille son téléphone. Dans ce cas, c'est bien le système d'exploitation qui délègue à France Identité la vérification locale de l'utilisateur, écartant ainsi toute confusion possible entre ces deux codes.

L'usager est alors pleinement enrôlé dans l'application mobile France Identité. Il peut utiliser son moyen d'identification électronique de niveau « faible » pour accéder à de nombreux services.

S'il souhaite disposer d'un niveau de garantie « élevé », l'usager devra compléter ce parcours par une vérification biométrique de son identité en mairie, dans le cadre de la procédure de certification dédiée.

1.1.7. *Certification en mairie de l'identité numérique*

Lorsqu'un usager active son identité numérique avec l'application France Identité, le niveau de garantie initial correspond au niveau « faible » au sens du règlement eIDAS. Ce niveau permet l'accès à de nombreux services en ligne. Pour certaines démarches nécessitant un niveau de confiance renforcé, l'usager peut élever ce niveau au niveau « élevé » grâce à une procédure de certification réalisée en mairie.

Cette certification repose sur une vérification d'identité effectuée en présence d'un agent habilité, dans une mairie équipée d'un dispositif approprié.

Demande de certification

L'usager initie sa demande depuis l'application France Identité. Il s'authentifie dans l'application et génère un code de demande lui permettant de se présenter en mairie muni de sa carte nationale d'identité électronique et de son smartphone. L'application l'informe des modalités pratiques de cette démarche.

Vérification de l'identité en mairie

Lors du rendez-vous, l'agent habilité procède aux contrôles nécessaires afin de s'assurer que la personne présente est bien la titulaire du titre. Ces vérifications reposent notamment sur la présentation du titre d'identité, sur des contrôles automatisés permettant d'en confirmer la validité ainsi que sur une comparaison biométrique réalisée localement à partir des données contenues dans le titre.

La vérification est réalisée localement à partir des données contenues dans le titre, sans constitution de traitement biométrique supplémentaire. Aucune donnée biométrique n'est transmise au système gérant l'identité numérique. Seul le résultat de la vérification est communiqué afin d'attester du niveau de garantie obtenu.

Transmission du résultat et activation

À l'issue du contrôle, le résultat de la certification est transmis de manière sécurisée au système concerné. Après notification de ce résultat, l'usager finalise l'activation de son identité numérique dans l'application en réalisant les actions d'authentification requises. Des vérifications complémentaires peuvent être effectuées afin de confirmer la cohérence du parcours et la validité du titre.

Une fois ces étapes validées, l'identité numérique est activée au niveau « élevé ». Ce niveau de garantie permet d'accéder à des démarches nécessitant une

vérification d'identité renforcée, équivalente, pour certains usages, à un contrôle en face-à-face.

Certification lors de la remise du titre

Dans certains cas, la certification peut être proposée directement lors de la remise du titre d'identité en mairie. L'usager est alors informé de cette possibilité et peut réaliser les démarches nécessaires selon un parcours simplifié. À l'issue des vérifications requises et après activation dans l'application, il bénéficie également d'une identité numérique de niveau « élevé ».

1.1.8. *Authentification à des services en ligne*

Le traitement SGIN a été historiquement conçu pour permettre à ses usagers de disposer d'un moyen d'identification électronique (MIE), au sens du règlement (UE) n° 910/2014 dit eIDAS.

Le MIE désigne tout élément matériel et/ou immatériel contenant des données d'identification personnelle, utilisé pour authentifier une personne physique auprès d'un service en ligne. France Identité, en reposant sur la CNIe, est le MIE régalien qui permettant aux usagers de prouver leur identité en ligne de façon sécurisée pour accéder à de nombreux services numériques, qu'ils soient publics ou privés.

Authentification avec FranceConnect

FranceConnect est un dispositif d'identification proposé par l'État permettant aux usagers de se connecter à de multiples services en ligne à l'aide d'une identité numérique unique. Lorsqu'un usager choisit France Identité comme fournisseur d'identité, il peut s'authentifier de manière sécurisée auprès des services compatibles.

Le niveau de garantie associé à l'authentification dépend du parcours réalisé par l'usager dans l'application. Conformément au règlement eIDAS, plusieurs niveaux de confiance existent. En pratique, l'identité numérique peut être utilisée avec un niveau de garantie « faible » ou « élevé ».

Les services ne nécessitant pas un niveau de confiance renforcé sont accessibles aux usagers ayant activé leur identité numérique. L'authentification s'effectue alors via FranceConnect.

Authentification avec FranceConnect+

Pour certains services impliquant des enjeux particuliers en matière de sécurité ou de protection des données, un niveau de garantie plus élevé est requis. Dans ce cas,

l'authentification s'effectue via FranceConnect+, la version du dispositif destinée aux usages nécessitant une vérification d'identité renforcée.

L'accès à FranceConnect+ est réservé aux usagers disposant d'une identité numérique préalablement certifiée. L'authentification repose sur des exigences de sécurité adaptées au niveau de garantie requis par le service.

Ce niveau de garantie permet notamment d'accéder à des démarches sensibles nécessitant une assurance renforcée quant à l'identité de la personne qui se connecte.

Authentification directe via le serveur SGIN

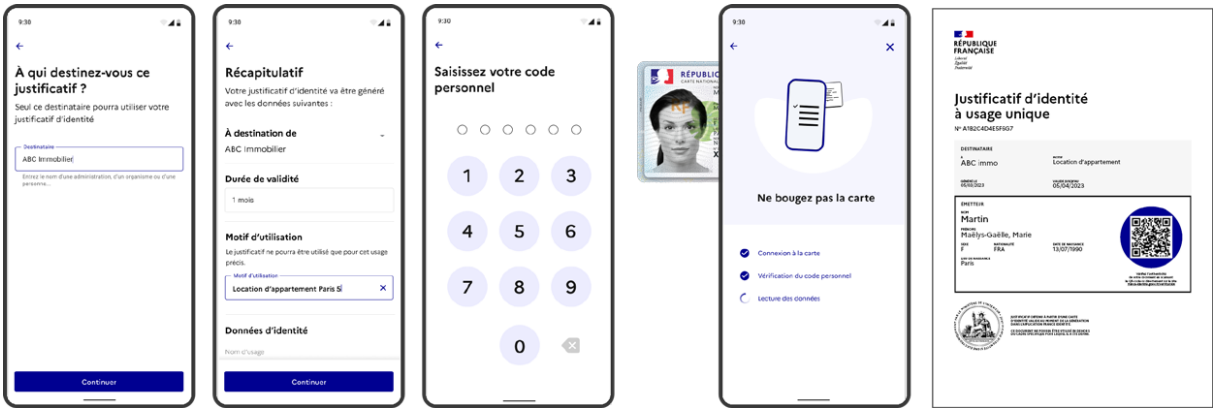
En complément de FranceConnect et FranceConnect+, certains services peuvent proposer une authentification via France Identité dans leurs propres parcours. Dans ce cadre, le SGIN agit comme fournisseur d'identité.

Ces services font l'objet d'un encadrement contractuel garantissant le respect des exigences applicables en matière de sécurité et de protection des données. Seules les informations strictement nécessaires à l'identification sont transmises, quel que soit le mode d'authentification retenu.

1.1.9. ***Attestation électronique d'identité***

L'application permet de générer une attestation électronique d'identité pouvant être présentée sous forme numérique ou partagée de manière dématérialisée. Cette attestation contient uniquement les informations nécessaires à la vérification de l'identité et intègre des dispositifs destinés à en garantir l'authenticité et l'intégrité.

L'attestation peut notamment être produite sous la forme d'un document électronique vérifiable, pouvant être transmis ou présenté lorsque la justification de l'identité est requise, dans des conditions assurant la protection des données personnelles.



La conservation des données

Données	Durées de conservation
Données d'identification issues du titre	Les attributs d'identité issus de la CNIe ne font l'objet d'aucune conservation côté serveur. Ces données sont utilisées uniquement pendant le temps nécessaire à la réalisation de l'opération, puis supprimées sans conservation. Seules les données dont la conservation est requise pour assurer la sécurité du service et le respect des obligations légales sont conservées pour des durées limitées. Ces attributs sont conservés localement sur le terminal de l'usager, sous son contrôle.
Données de l'attestation d'attributs d'identité	Aucune conservation par le SGIN. Conservées localement sur le terminal de l'usager dans l'identité dérivée (dans le terminal de l'usager, sous son contrôle). Peuvent être utilisées temporairement lors de la génération d'attestation ou d'une authentification, mais sont supprimées immédiatement après traitement.

1.1.10. *Les accédants et les destinataires des données à caractère personnel des usagers*

Dans le cadre du traitement SGIN, l'accès aux données à caractère personnel est strictement encadré. Les accédants et les destinataires sont répartis selon les finalités du traitement.

Les Accédants internes au traitement (agents ou systèmes ayant accès aux données)
Les systèmes d'information habilités du responsable de traitement
Des prestataires techniques peuvent intervenir pour des opérations de maintenance dans un cadre strictement encadré, sans accès aux données d'identité

Des dispositifs de signature électronique mis en œuvre par l'État permettent de garantir l'authenticité des attestations.

Destinataires externes (personnes physiques ou morales recevant les données dans le cadre d'un usage autorisé
Usager (personne concernée) Accède aux données contenues dans sa propre carte d'identité et à l'attestation générée, via l'application France Identité. Il est le seul à pouvoir initier les opérations (authentification, génération d'attestation, export PDF).
Fournisseurs de services raccordés au SGIN Ces services publics ou privés, après signature d'une convention avec l'ANTS, peuvent recevoir les attributs d'identité nécessaires à l'identification ou à la vérification d'identité. Chaque fournisseur reçoit uniquement les données strictement nécessaires au service demandé, selon les règles définies dans la convention de raccordement.
Destinataires de l'attestation d'identité générée Toute entité physique ou morale choisis par l'usager et acceptant une attestation électronique d'attributs d'identité en tant que justificatif d'identité peut la consulter. Ces destinataires n'ont pas d'accès à l'ensemble du traitement, uniquement aux données figurant sur l'attestation remise par l'usager.

2. Étude des principes fondamentaux

2.1. Évaluation des mesures garantissant la proportionnalité et la nécessité du traitement

2.1.1. *Explication et justification des finalités*

Finalités	Légitimité
Mise à disposition d'un moyen d'identification électronique régalien Le SGIN permet aux titulaires d'une carte nationale d'identité électronique de s'identifier et de s'authentifier auprès	La légitimité des finalités du traitement SGIN repose essentiellement sur le décret n° 2022-676 du 26 avril 2022, qui autorise la création du Service de Garantie de l'Identité Numérique en tant

d'organismes publics ou privés via une application mobile.	que moyen d'identification électronique régalien et habilite l'État à traiter les données à caractère personnel nécessaires à ces finalités La finalité relative à l'intégration d'un portefeuille européen d'identité numérique s'inscrit, quant à elle, dans le cadre plus général de la mission d'intérêt public confiée à l'ANTS par le décret n° 2007-240 du 22 février 2007 (modifié le 26 février 2024) et répond aux objectifs de simplification, de sécurité et de transition numérique du service public.
Génération d'attestations électroniques d'attributs d'identité L'application offre à l'usager la possibilité de générer des attestations électroniques ne comportant que les attributs d'identité nécessaires et choisis par l'usager.	
Interopérabilité européenne et intégration du Portefeuille d'Identité Numérique Européen (EUDI Wallet) Assurer la compatibilité du SGIN avec les exigences du règlement eIDAS 2 et le cadre d'architecture du portefeuille EUDI, en facilitant l'échange sécurisé d'attributs qualifiés à l'échelle de l'Union européenne.	

2.1.2. *Explication et justification du fondement*

Au regard de l'article 6 du RGPD, la licéité du traitement est assurée si au moins une des conditions suivantes est remplie :

Critères de licéité	Applicable	Justification
Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.	***Non***	Le SGIN n'est pas mis en œuvre pour satisfaire une obligation légale pesant directement sur l'ANTS.
Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement (6 (1e) RGPD).	***Oui***	Le traitement SGIN est mis en œuvre par l'ANTS dans le cadre de sa mission d'intérêt public instituée par le décret n° 2022-676 du 26 avril 2022, qui définit expressément le Service de Garantie de l'Identité Numérique comme un service public relevant de l'exercice de l'autorité publique et habilite l'État à traiter les données à caractère personnel nécessaires à ces finalités. Cette base de licéité s'inscrit également dans le périmètre des missions dévolues à l'ANTS par le décret n° 2007-240 du 22 février 2007, tel que modifié par le décret n° 2024-146 du 26 février 2024, qui confère à l'Agence la responsabilité générale des titres sécurisés et des services d'identité numérique de l'État, justifiant ainsi la licéité du traitement SGIN au titre de l'exécution d'une mission d'intérêt public.

Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique.	***Non***	***/***
La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ou traitement.	***Non***	***/***
Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci.	***Non***	***/***

2.1.3. *Explication et justification de la minimisation des données*

Le traitement des attributs dans le cadre du SGIN respecte le principe de minimisation. L'article 5(1)(c) du RGPD dispose à ce titre, que les données collectées doivent être *"adéquates, pertinentes et limitées à ce qui est nécessaire aux fins pour lesquelles elles sont traitées"*.

- **Collecte strictement ciblée :** Les usagers initient eux-mêmes la demande des attributs qu'ils souhaitent voir figurer sur leur attestation (âge, droits à conduire, diplômes, etc.), garantissant que seules les données indispensables à la finalité sollicitée sont extraites et traitées.

- **Politique de non-conservation des données personnelles :** Les attributs d'identité transitent via le serveur SGIN uniquement pour réaliser la transaction demandée, puis sont supprimés sans conservation ultérieure. Aucune donnée d'identité n'est

stockée sur le serveur au-delà de la durée strictement nécessaire à l'authentification de la personne concernée ou de la génération de l'attestation.

- **Stockage local sécurisé :** Les seules données conservées sur le smartphone sont celles extraites du composant électronique du titre, sous le contrôle exclusif de l'usager.

- **Divulgation sélective et usage unique** : Le traitement permet de générer des attestations à usage unique ou à contenu restreint, limitant la portée des données partagées aux tiers et évitant toute collecte superflue ou réutilisation abusive.

Détail des données traitées	Catégories	Justification du besoin et de la pertinence des données	Mesures de minimisation
• Nom, • Prénoms, • Date naissance, • Libellé du lieu naissance • Nationalité, • Sexe, • Photographie, • Adresse,	Données d'identité extraites de la CNIe, (art. 2 décret SGIN)	Nécessaires pour l'authentification de l'usager, la génération sécurisée d'attestations conformes aux exigences eIDAS et au décret SGIN. La photographie peut être utilisée pour la génération de l'attestation d'identité et n'est pas utilisée pour l'authentification.	Lecture restreinte à ces seuls champs ; Suppression aussitôt la transaction effectuée ; Stockage chiffré dans le terminal de l'usager
• Numéro du titre	Donnée extraite de la CNIe, (art. 2 décret SGIN)	Permet d'identifier de manière univoque le titulaire du moyen d'identification électronique et de	En principe, cinq (5) ans sur le serveur à compter de la dernière utilisation du moyen

		corréler les opérations à l'usager concerné dans les journaux. Cette référence est nécessaire pour répondre à une réquisition judiciaire et pour instruire toute demande d'exercice des droits RGPD (accès, effacement, rectification).	d'identification (art. 4 I du décret SGIN) **Toutefois, une purge automatique du numéro de document est réalisé au bout de trois (3) ans, simultanément avec les logs d'opérations (alignement sur l'article 5 du Décret SGIN).**
• Logs d'authentification et d'opérations • Identifiant usager, date/heure, type d'opération, horodatage	Données de journalisation	Garantir auditabilité, détection des incidents et traçabilité requises par l'ANSSI	Conservation limitée à trois (3) ans maximum sur serveur (art. 5 décret SGIN) puis purge automatique

Procédure 1 - Authentification sécurisée :
Les données d'identification extraites de la carte nationale d'identité électronique, permettent d'authentifier l'usager de manière sécurisée auprès des Fournisseurs de services, assurant ainsi que l'accès aux services et données est légitimement accordé à la personne concernée.

Procédure 2 - Génération d'attestations d'identité :
Les données d'identification servent à générer une attestation électronique d'identité valide qui peut être utilisée pour des démarches administratives ou légales.

Ces deux processus sont mis en œuvre en conformité avec les réglementations sur la protection des données, assurant un traitement des données personnelles transparent, sécurisé et limité aux nécessités fonctionnelles du service.

2.1.4. *Explication et justification de la qualité des données*

Mesures pour la qualité des données	Modalités de mise en œuvre
Fiabilité des données	Les données d'identité (nom, prénoms, nom d'usage, sexe, date et lieu de naissance, nationalité, photographie, adresse, numéro du titre) proviennent directement du composant électronique de la CNIe, délivrée et signée par l'ANTS.
Intégrité des données	La lecture des données s'effectue via un canal sécurisé vers le terminal de l'usager, où chaque attribut est vérifié grâce à la signature numérique du composant électronique, garantissant qu'aucune altération n'a eu lieu depuis l'émission de la CNIe.
La qualification de la responsabilité du traitement	L'ANTS est exclusivement responsable du traitement des données visant à permettre aux usagers d'accéder aux services en lignes partenaires et de générer des attestations électroniques d'identité sur demande.

Types de données	Durée de conservation	Justification de la durée de conservation	Mécanisme de suppression à la fin de la conservation
Données d'identification issues de la Carte Nationale d'Identité Électronique (CNIe) Nom, prénoms, nom d'usage, sexe, date & lieu de naissance, nationalité, photographie, adresse, numéro de document	Les données d'identification sont uniquement utilisées durant la session active pour authentifier l'usager et permettre la génération de l'attestation électronique.	Principe de minimisation qui garantit que les informations ne sont pas stockées au-delà de la durée nécessaire pour accomplir la finalité spécifique de traitement.	Pendant la session active, les données ne sont exploitées que pour authentifier l'usager et générer l'attestation. Elles sont supprimées sitôt la transaction réalisée.

Enregistrements des opérations sur le MIE Création, consultation, utilisation, révocation, suppression ; identifiant auteur, date, heure, objet, numéro de document	Trois (3) ans à compter de la date de chaque enregistrement (art. 5 du décret SGIN)	Garantit la traçabilité et l'auditabilité des opérations liées à chaque document, nécessaire pour gérer d'éventuels contentieux, réquisitions judiciaires et l'exercice des droits au titre du RGPD, sans prolonger indûment la conservation.	Suppression automatique via tâche planifiée dès l'expiration du délai de trois (3) ans.
Journaux de connexion issus du Système informatique SGIN	Trois (3) ans à compter de la date de chaque enregistrement (art. 5 du décret SGIN)	Répond aux exigences de sécurité opérationnelle : audits réguliers, détection et investigation des incidents, conformité réglementaire (CNIL, ANSSI).	Mesures de sécurité (chiffrement, accès restreint) durant la conservation, puis suppression automatique des journaux au-delà de trois (3) ans.
Attestation électronique d'attributs d'identité (fichier PDF ou mdoc généré par l'usager)	Durée fixée par l'usager lors de la génération, dans la limite de trois (3) mois maximum	Limitation du risque de réutilisation malveillante par un tiers, conformément aux principes de minimisation, de finalité et de durée prévus par le RGPD	L'attestation est stockée localement sur le terminal de l'usager. À l'issue de la durée définie, elle devient automatiquement invalide et ne peut plus être vérifiée. L'usager peut la supprimer manuellement.

2.1.5. *Évaluation des mesures*

Mesures garantissant la proportionnalité et la nécessité du traitement	Acceptable / améliorable
Finalités : déterminées, explicites et légitimes	***Acceptable***
Fondement : licéité du traitement	***Acceptable***
Minimisation des données : adéquates, pertinentes et limitées	***Acceptable***
Qualité des données : exactes et tenues à jour	***Acceptable***
Durées de conservation : limitées	***Acceptable***

2.2. Évaluation des mesures protectrices des droits des personnes concernées

2.2.1. *Détermination et description des mesures pour l'information des personnes*

Mesures pour le droit à l'information	Modalités de mise en œuvre et justifications
Présentation des conditions de confidentialité	Politique de protection des données facilement accessible par un lien permanent dans l'application ou sur le site internet france-identite.gouv.fr. Document actualisé à chaque évolution réglementaire ou technique. Garantit la transparence et l'accès continu à l'information sur la gestion des données (finalités, bases légales, durées de conservation, droits).
Conditions lisibles et compréhensibles	Ces documents sont rédigés en termes clairs et précis, assurant ainsi leur compréhensibilité. Ces mentions sont détaillées de manière accessible, afin que chaque utilisateur comprenne pleinement ses droits et les pratiques de traitement de ses données personnelles.
Présentation détaillée des finalités des traitements de données (objectifs précis, croisements de données s'il y a lieu, etc.)	La Politique de protection des données présente pour chaque finalité, les catégories de données conservées et les durées de conservation correspondantes.
Présentation des droits de la personne concernée	**La Politique de protection des données** définit les droits dont disposent les personnes sur les données traitées et les moyens de les exercer.

	Droit à l'information : Les usagers peuvent obtenir des informations détaillées sur le traitement de leurs données en contactant l'ANTS. **Droit d'accès :** Les données d'identité contenues dans la puce électronique ne sont pas conservées par le SGIN et sont automatiquement supprimées à la fin de chaque transaction. Toutefois, un droit d'accès peut s'exercer sur le numéro du titre et sur les traces d'utilisation de l'application France Identité. Le numéro du titre est conservé afin de permettre à la personne concernée d'exercer une demande d'accès ou afin de répondre à une réquisition judiciaire. **Droit de rectification :** L'usager a le droit d'obtenir la rectification des données à caractère personnel le concernant qui sont inexactes ou incomplètes. Toutefois, l'ANTS n'est pas habilitée à répondre aux demandes de rectification concernant les données provenant des fournisseurs d'attributs partenaires. Les usagers souhaitant exercer ce droit doivent s'adresser directement à l'administration partenaire, qui a fourni les données. **Droit d'opposition :** Conformément à l'article 21 du RGPD, l'usager peut exercer son droit d'opposition. L'exercice de ce droit implique la désinstallation de l'application France Identité, ce qui entraîne automatiquement la suppression des données stockées sur le serveur et sur le terminal de l'usager, à l'exception de celles conservées à des fins de résolution d'éventuels contentieux.
Modalités de contact (identité et coordonnées).	La Politique de protection des données donne les coordonnées du responsable du traitement SGIN et de son délégué à la protection des données.

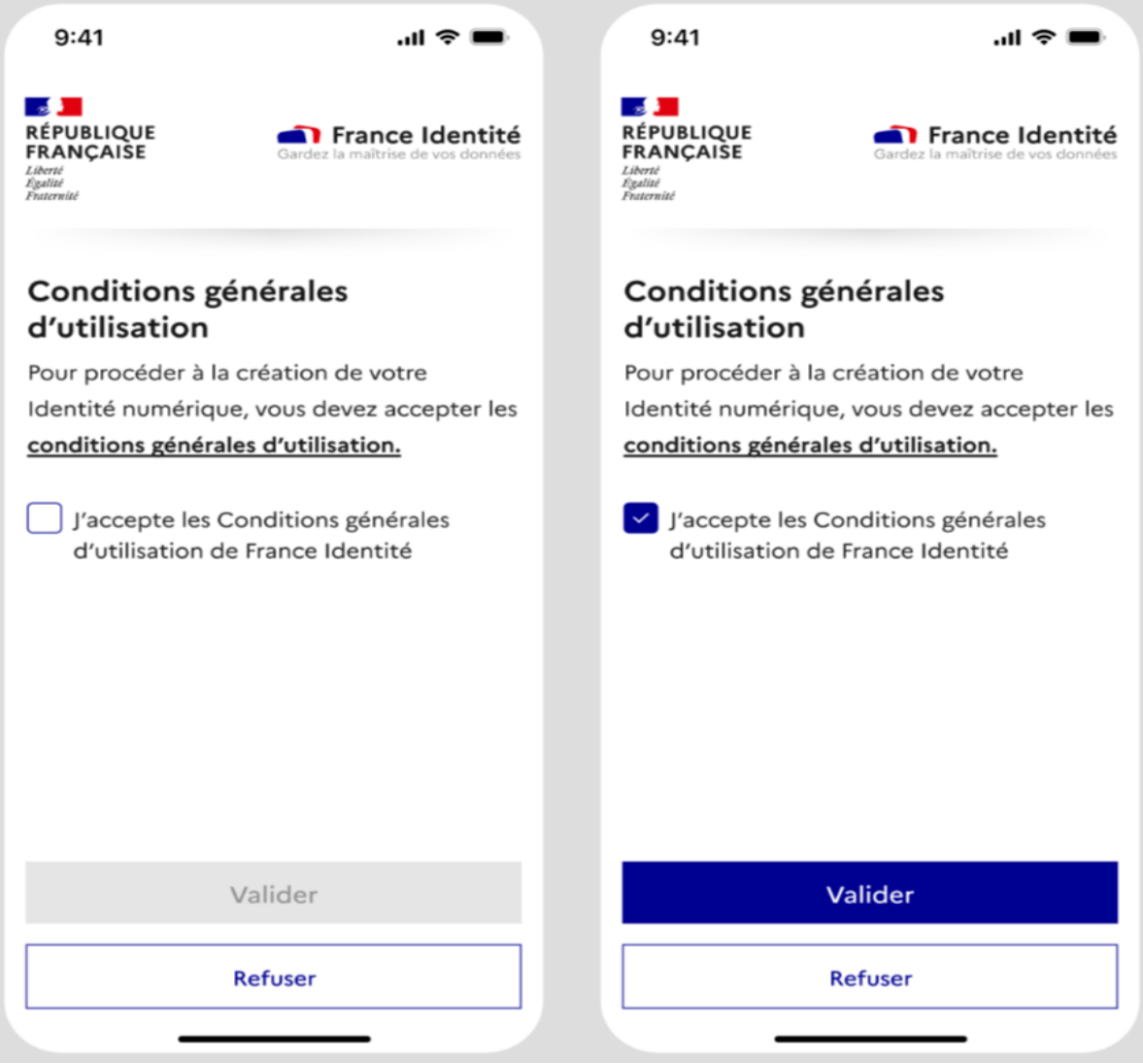
Le cas échéant, information de la personne concernée de tout changement concernant les données collectées, les finalités, les clauses de confidentialité	La Politique de protection des données est accessible aux utilisateurs à cette adresse et elle est actualisée à chaque modification du traitement. La responsabilité du traitement SGIN est assurée conjointement par le secrétariat général du ministère de l'intérieur et par l'agence nationale des titres sécurisés (ANTS), établissement public à caractère administratif placé sous tutelle du ministère de l'intérieur. Toute évolution concernant le statut des deux responsables de traitement identifiés donne lieu à une actualisation des mentions d'information.
Dans le cas de transmission de données à des tiers :	**Sans objet**
Présentation détaillée des finalités de transmission à des tiers	Le détail des informations est précisé dans la Politique de protection des données.
Présentation détaillée des données personnelles transmises	
Indication de l'identité des entreprises tierces	

2.2.2. *Détermination et description des mesures pour le recueil du consentement*

Au moment où l'usager engage chacune des trois principales interactions (« ouverture de l'application », « authentification auprès d'un service en ligne », « génération d'une attestation »), l'application France Identité informe utilisateur du traitement de ces données personnelles selon les 3 modalités suivantes :

a. Ouverture de l'application et acceptation des CGU et de la Politique de confidentialité

Lors de la toute première ouverture de France Identité, une page d'accueil à l'écran impose la lecture et l'acceptation explicite des Conditions Générales d'Utilisation et de la Politique de protection des données. L'usager ne peut poursuivre sans avoir coché la case ***« J'ai lu et j'accepte les CGU et la Politique de confidentialité »***. Cet acte atteste que l'utilisateur a pris connaissance des Conditions Générales d'Utilisation et de la Politique de confidentialité, sans pour autant, à ce stade, constituer un consentement légal au traitement des données, lequel repose pour le SGIN sur une mission d'intérêt public (art. 6 § 1 e RGPD).



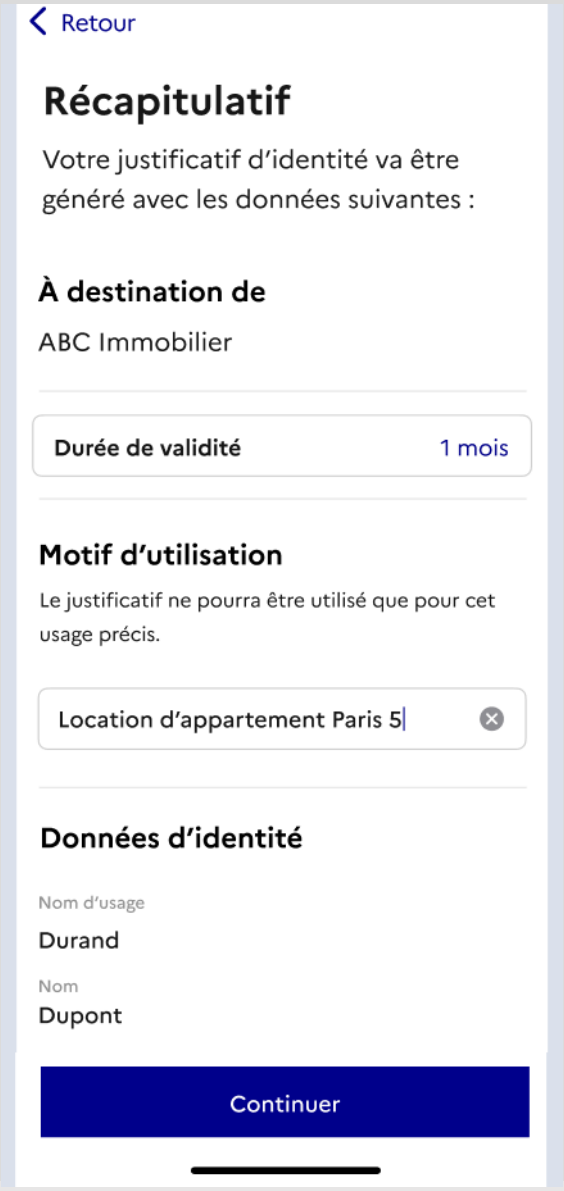
b. Acceptation à la transmission des données auprès d'un service en ligne

Lorsque l'usager choisit de s'authentifier auprès d'un service externe une fenêtre modale contextualise le transfert sécurisé de ses données d'identité extraites de la puce de la CNIe. L'écran rappelle les catégories de données lues, et invite l'utilisateur à cliquer sur ***« Accepter »*** pour confirmer qu'il accepte la transmission de ces données au fournisseur de service tiers. En cas de refus, la connexion est interrompue et l'usager reste sur l'application France Identité.

c. Information du traitement de la création d'une attestation électronique d'identité

Avant de générer son attestation d'identité, l'utilisateur est présenté à nouveau avec une modalité d'information spécifique à l'attestation. Ce dialogue décrit la finalité du traitement, soit la génération sécurisée du document et les données utilisées. Le refus entraîne l'impossibilité de générer l'attestation.

Cette procédure garantit que les usagers comprennent qu'ils initient eux-mêmes la transmission de leurs données pour un objectif précis. Il leur est clairement indiqué que leurs données seront exclusivement traitées pour les besoins du traitement.



2.2.3. *Détermination et description des mesures pour les droits d'accès*

Mesures pour le droit d'accès	Modalités de mise œuvre
Le droit d'accès (article 15 du RGPD) consiste en la possibilité d'accéder à l'ensemble des données à caractère personnel. Les usagers peuvent soumettre une demande formelle pour accéder aux données que le traitement SGIN détient à leur sujet.	L'Agence nationale des titres sécurisés (ANTS), responsable du traitement SGIN, authentifie les usagers auprès des services en ligne partenaires sans conserver durablement leurs données d'identité. Conformément à la Politique de confidentialité de France Identité, les attributs extraits de la puce de la CNIe (nom, prénoms, date et lieu de naissance, etc.) sont lus uniquement en mémoire vive pendant la session active, puis immédiatement purgés. Aucune donnée personnelle n'est stockée sur les serveurs de l'ANTS. Seules des données techniques et de journalisation sont conservées pour des durées limitées conformément aux textes applicables. Les demandes d'exercice du droit d'accès peuvent être adressées à l'ANTS à cette adresse électronique : contact@franceidentite.gouv.fr Seuls les journaux d'événements techniques et fonctionnels (connexions, opérations sur le moyen d'identification) sont conservés trois ans puis supprimés automatiquement à l'issue de cette période. Les données d'identité issues de la CNIe peuvent transiter via le serveur pour effectuer la transaction, mais ne font pas l'objet d'une conservation au-delà de la session. La génération d'attestation n'entraîne pas de stockage de données éphémères, qui sont purgées dès la fin de l'opération.

	En conséquence, toute demande d'accès portant sur des informations conservées au-delà des durées légales ou concernant des données non stockées ne pourra aboutir.

2.2.4. *Détermination et description des mesures pour les droits de rectification*

Mesures pour le droit de rectification	Modalités de mise œuvre
La mise en œuvre de ce droit permet de rectifier des informations inexactes ou incomplètes (articles 16 et 19 du RGPD).	L'ANTS, en tant que responsable du traitement SGIN, ne traite que les données strictement nécessaires à l'authentification de l'usager et à la génération d'attestations d'identité. Les attributs fournis par les administrations ou entités partenaires (notamment via France Connect) sont lus uniquement pour réaliser la transaction puis immédiatement supprimés. L'ANTS ne les conserve pas au-delà de cette opération et n'est pas compétente pour en assurer la rectification. Pour toute demande de correction d'un attribut, par exemple le nom ou la date de naissance, l'usager doit s'adresser directement à l'administration ou à l'entité qui a fourni ces données. **En conséquence, l'ANTS n'est pas habilitée à répondre aux demandes de rectification concernant des données tierces et les usagers souhaitant exercer ce droit doivent contacter la source d'origine.**

2.2.5. *Détermination et description des mesures pour les droits de limitation du traitement et droit d'opposition*

Mesures pour le droit d'opposition	Modalités de mise œuvre
L'usager peut s'opposer à tout moment au traitement des données le concernant, en justifiant de raisons tenant à sa situation particulière (article 21 du RGPD).	La désinstallation de l'application met fin à l'usage et entraîne la suppression des données conservées sur le terminal. Les données conservées le sont uniquement pour des finalités déterminées et pour les durées prévues par les textes applicables.

2.2.6. *Détermination et description des mesures pour la sous-traitance*

Le responsable du traitement s'appuie, lorsque cela est nécessaire, sur des sous-traitants intervenant notamment dans le cadre de l'hébergement, de la maintenance et de l'exploitation du système d'information.

Conformément à l'article 28 du règlement (UE) 2016/679, ces sous-traitants sont sélectionnés pour leurs garanties en matière de sécurité et de protection des données à caractère personnel. Leur intervention est strictement encadrée par des contrats définissant précisément l'objet du traitement, sa durée, sa nature, les catégories de données concernées ainsi que les obligations de confidentialité et de sécurité qui leur incombent.

Le responsable du traitement veille à ce que les sous-traitants n'agissent que sur instruction documentée et met en œuvre des mécanismes de contrôle destinés à s'assurer du respect de leurs obligations.

Aucun sous-traitant n'est autorisé à recourir à un sous-traitant ultérieur sans autorisation préalable, spécifique ou générale, du responsable du traitement, dans les conditions prévues par le RGPD.

2.2.7. *Détermination et description des mesures pour le transfert de données en dehors de l'Union européenne*

Les données à caractère personnel collectées et traitées dans le cadre du traitement SGIN ne font l'objet d'aucun transfert hors de l'Union-Européenne.

2.2.8. *Évaluation des mesures*

Mesures protectrices des droits des personnes concernées	Acceptable / Améliorable	Mesures correctives
Information des personnes concernées (traitement loyal et transparent)	***Acceptable***	***N/A***
Recueil du consentement	***N/A***	***N/A***
Exercice des droits d'accès	***N/A***	***N/A***
Exercice des droits de rectification et d'effacement	***N/A***	***N/A***
Exercice des droits à la limitation du traitement et d'opposition	***N/A***	***N/A***
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	***N/A***	***N/A***

3. Validation de l'analyse

3.1. Synthèse de la conformité au RGPD des mesures permettant le respect des principes fondamentaux

Finalités	Évaluation
Finalités : déterminées, explicites et légitimes	***Acceptable***
Fondement : licéité du traitement, interdiction du détournement de finalité	***Acceptable***
Minimisation des données : adéquates, pertinentes et limitées	***Acceptable***
Qualité des données : exactes et tenues à jour	***Acceptable***
Durées de conservation : limitées	***Acceptable***
Information des personnes concernées (traitement loyal et transparent)	***Acceptable***
Recueil du consentement	***Acceptable***
Exercice des droits d'accès et à la portabilité	***N/A***
Exercice des droits de rectification et d'effacement	***N/A***
Exercice des droits à la limitation du traitement et d'opposition	***N/A***
Sous-traitance : identifiée et contractualisée	***Acceptable***
Transferts : respect des obligations en matière de transfert de données en dehors de l'Union européenne	***N/A***