Analyse d'impact relative à la protection des données
-
Service de garantie de l'identité numérique (SGIN)

Informations sur l'analyse d'impact

Nom du traitement
Service de garantie de l'identité numérique - SGIN

Responsables du traitement
Le ministère de l'intérieur (respire général)
L'Agence nationale des titres sécurisés (ANTS)

Service gestionnaire : Programme interministériel France identité numérique

Nom de l'auteur de l'analyse d'impact
Direction du programme interministériel France identité numérique - Ministère de l'intérieur

Nom du délégué à la protection des données
Fabrice Mattatia – Délégué à la Protection des Données - Ministère de l'intérieur

Date de création
27/08/2021

Table des matières

Définitions

Identification électronique : processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale[1].

Moyen d'identification électronique : élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne[2].

Authentification : processus électronique qui permet de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique[3].

Données d'identité : elles 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.

***Ordiphone* :** téléphone portable ou *smartphone* sur lequel l'usager télécharge l'application mobile. L'*ordiphone* doit :

- opérer avec un système d'exploitation Android dans une version compatible ou un système d'exploitation iOS dans une version compatible ;
- être doté d'un lecteur NFC.

[1] Article L. 102 du code des postes et des communications électroniques et article 3. 1) du règlement n 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement « eIDAS ».
[2] Article L. 102 du code des postes et des communications électroniques et article 3. 2) du règlement « eIDAS ».
[3] Article 3. 5) du règlement eIDAS.

Avant-propos : contexte et enjeux de l'identité numérique régalienne

A. Un besoin croissant de sécurisation des identités en ligne

Les démarches dématérialisées font aujourd'hui l'objet d'un usage massif. Ainsi, dans le dernier sondage effectué pour le compte de la direction du programme interministériel France identité numérique en 2020[4] :

- 78 % des personnes interrogées déclarent effectuer des opérations commerciales et bancaires en ligne au moins une fois par mois ;
- 80 % d'entre elles déclarent procéder à leurs démarches administratives en ligne.

Dans ce contexte, encore accentué par la crise sanitaire, le besoin d'identification et d'authentification numériques est croissant et constitue l'un des facteurs de confiance déterminants pour la poursuite du développement de cet écosystème digital.

La simplification, la maîtrise et la sécurisation de leur identité numérique deviennent dès lors un enjeu quotidien pour les usagers, par ailleurs de plus en plus souvent victimes d'usurpation d'identité en ligne. Ainsi, dans le même sondage :

- plus d'une personne interrogée sur quatre déclare avoir fait l'objet d'une ou plusieurs tentatives de vol de son identité en ligne au cours de ces deux dernières années ;
- près d'une sur cinq déclare avoir été effectivement victime d'une usurpation d'identité en ligne.

Dans son rapport d'information du 8 juillet 2020[5], l'Assemblée nationale souligne les fortes attentes en la matière : « *L'identité numérique, c'est-à-dire la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources, est un projet décisif pour la France et les Français. Dans notre ère résolument numérique, les citoyens utilisent en effet de plus en plus l'internet pour réaliser les tâches de leur vie quotidienne, qu'il s'agisse d'inscrire leurs enfants à l'école, d'acheter des biens et des services, ou encore d'accéder à des services publics de plus en plus dématérialisés. Ils ont donc besoin d'un moyen simple et sécurisé de prouver leur identité en ligne, tout comme, dans l'espace physique, ils peuvent recourir à leur titre d'identité physique (carte nationale d'identité, passeport) afin de prouver leur identité dans les situations où cela s'avère nécessaire.* »

B. L'Etat, garant de l'identité dans le monde numérique

A l'instar du monde physique, l'Etat apparaît comme le garant de l'identité des citoyens dans le monde numérique. Dans son rapport de juin 2020[6], le Conseil national du numérique (CNum) indique à ce titre que l'identité numérique régalienne est la « *clef de voûte de la citoyenneté numérique* ». Il plaide pour que *« l'identité numérique régalienne soit appréhendée et conçue en tant que service public à part entière, engageant dans ses principes les valeurs de protection de l'usager, de frugalité des données, de confiance et d'égalité de tous les citoyens dans l'accès aux droits et à la puissance publique*. »

[4] Sondage IPSOS été 2020 portant sur un échantillon de 4 000 personnes, âgées de 18 ans et plus, et représentatives de la population française.
[5] Mission d'information commune sur l'identité numérique, Rapport d'information n 3190 du 8 juillet 2020.
[6] Conseil national du numérique, *Identités numériques. Clés de voûte de la citoyenneté numérique*, juin 2020.

La CNIL, elle-même, dans sa délibération du 11 février 2021[7] portant notamment sur le projet de décret modifiant le décret relatif à la carte nationale d'identité estime « *que la mise en œuvre d'une identité numérique d'Etat de haut niveau, respectueuse des principes* « Informatique et Libertés »*, doit être encouragée. Elle considère à ce titre que la mise en œuvre d'une carte nationale d'identité électronique (CNIe) a vocation à répondre à des usages régaliens (document de voyage, preuve d'identité lors de contrôles, lutte contre la fraude documentaire) qui font l'objet du projet de décret soumis à la Commission, mais également, à terme, à des services d'identité numérique.* »

C. La mission de la direction du programme interministériel France identité numérique

Dès 2018, l'Etat s'est engagé dans la préparation d'un dispositif d'identité numérique, au travers de la mise en place, à la demande du Premier ministre, par le ministre de l'intérieur, la ministre de la justice et le secrétaire d'Etat au numérique, du programme « France Identité Numérique ».

Ainsi, aux termes de deux lettres de mission du 5 janvier 2018 et du 2 août 2019, confirmées par des réunions interministérielles successives, la direction du programme interministériel France identité numérique s'est vu confier la charge de mettre à la disposition du public une identification électronique sécurisée s'appuyant sur les titres pourvus d'un composant électronique et en particulier sur la nouvelle carte d'identité, répondant aux exigences les plus élevées du règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, dit règlement « eIDAS », dans l'objectif de lutter contre « *le risque d'utilisation abusive ou d'altération de l'identité* », et facile d'utilisation.

Plus précisément, l'article 8 du règlement eIDAS définit trois niveaux de garantie s'appliquant aux moyens d'identification électronique :

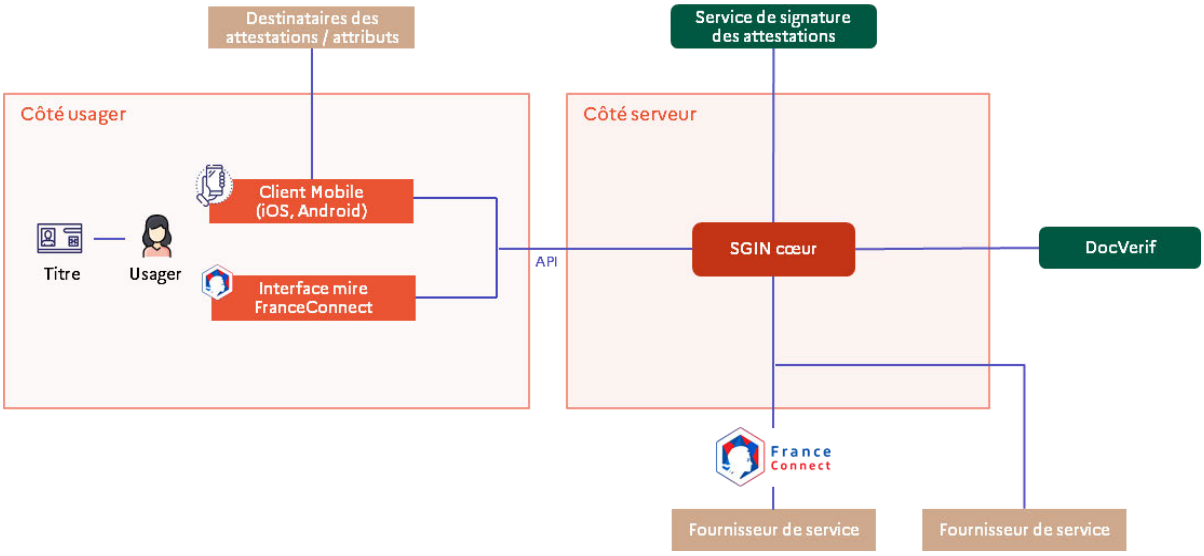
- le niveau de garantie faible renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré limité de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie substantiel renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un degré substantiel de fiabilité à l'identité revendiquée ou prétendue d'une personne, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité ;
- le niveau de garantie élevé renvoie à un moyen d'identification électronique dans le cadre d'un schéma d'identification électronique qui accorde un niveau de fiabilité à l'identité revendiquée ou prétendue d'une personne plus élevé qu'un moyen d'identification électronique ayant le niveau de garantie substantiel, et est caractérisé sur la base de spécifications techniques, de normes et de procédures y afférents, y compris les contrôles techniques, dont l'objectif est d'empêcher l'utilisation abusive ou

[7] Délibération n 2021-022 du 11 février 2021 portant avis sur un projet de décret modifiant le décret n 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité et le décret n 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

l'altération de l'identité. Ce dernier niveau emporte, selon le projet de décret d'application, la présomption de fiabilité prévue par l'article L. 102 du code des postes et des communications électroniques.

Ce dispositif, le « service de garantie de l'identité numérique » ou SGIN, constitue un « moyen d'identification électronique » au sens du règlement eIDAS.

D. Schéma d'architecture générale du service de garantie de l'identité numérique (SGIN)



E. Les principes de conception du SGIN

La conception du moyen d'identification électronique régalien obéit à un certain nombre de principes, afin de répondre aux exigences des lettres de mission et à en faciliter l'adoption par le grand public.

- L'autonomie de l'usager

L'objectif du futur moyen d'identification électronique est de permettre aux usagers qui ont choisi d'en bénéficier de maîtriser l'utilisation et la diffusion de leurs données d'identité. Pour ce faire, il repose essentiellement sur l'association d'un titre d'identité (carte nationale d'identité disposant d'un composant électronique) en cours de validité, d'un code secret et d'un *ordiphone* (c'est-à-dire d'un téléphone portable), tous trois sous le contrôle des usagers.

Par ailleurs, il convient de rappeler que ce moyen d'identification électronique régalien sera facultatif. Il constitue donc un service optionnel mis à la disposition des usagers.

Enfin, que les usagers décident ou non de disposer d'un moyen d'identification électronique proposé par l'Etat, ils conserveront la possibilité de recourir à d'autres dispositifs d'authentification électronique (comme, par exemple, le moyen d'identification électronique de niveau de garantie substantiel proposé par la Poste) ou d'entrer en contact avec les organismes publics ou privés par des voies autres qu'électroniques (par exemple, la possibilité de se rendre sur place aux guichets).

- La simplicité d'utilisation

L'ergonomie, l'accessibilité et l'inclusivité du futur moyen d'identification électronique de l'Etat sont, au même titre que la sécurité, prioritaires dans son cahier des charges. C'est à ce titre que le choix a été fait, à la différence du prototype ALICEM, de ne pas recourir à un dispositif de vérification d'identité à distance (ou reconnaissance faciale) mais de s'appuyer uniquement sur une procédure de vérification d'identité en face-à-face.

Par ailleurs, le recrutement de deux UX designers[8], dès le lancement du programme, atteste de du souci constant d'ergonomie.

Enfin, le cahier des charges du marché de développement du moyen d'identification électronique régalien intègre les référentiels en matière d'accessibilité : il est ainsi conforme à l'arrêté du 20 septembre 2019 portant référentiel général d'amélioration de l'accessibilité (RGAA) qui définit notamment les modalités techniques d'accessibilité des services en ligne de l'État sur le Web et la téléphonie.

- La minimisation de la collecte des données à caractère personnel

Les seules données d'identité utilisées sont celles figurant sur le titre d'identité physique. Les données correspondantes, extraites du composant électronique du titre sont conservées uniquement localement (dans une zone protégée de l'*ordiphone*[9]), sous le seul contrôle des usagers.

Le serveur du SGIN, nécessaire pour le bon fonctionnement du système et notamment l'authentification du titre et la transmission des données d'identité aux fournisseurs de services, ne contient pas de données d'identité extraites de ce composant électronique. Les données d'identité, devant être transmises aux fournisseurs de téléservices ou devant figurer sur les attestations électroniques d'attributs d'identité ou d'un attribut d'identité, transitent *via* le serveur du SGIN uniquement pour permettre la réalisation des transactions concernées. Elles en sont supprimées sitôt ces transactions réalisées. Par ailleurs, lorsque les transactions consistent en l'apport de la preuve de l'âge ou de la majorité par affichage sur l'écran de l'*ordiphone* des usagers, le serveur du SGIN n'est jamais sollicité.

Enfin, le dispositif peut permettre la divulgation sélective des données d'identité en fonction des besoins des usagers (par exemple, obtention d'une attestation électronique d'un attribut d'identité pour apporter la preuve de l'âge ou de la majorité des usagers).

- La transparence

La solution d'identité numérique est développée en recourant autant que possible à des ressources en *open source*, de façon à ce que son code source puisse être librement consulté par le public conformément aux dispositions du code des relations entre le public et l'administration[10] sous réserve d'avoir les garanties de sécurité suffisantes (sensibilité des fonctionnalités, audit de sécurité, réalisation du *bug bounty*, etc.) et que la solution soit déployée en production. Ce choix, conforme aux objectifs gouvernementaux[11], est apparu comme nécessaire pour assurer une pleine confiance des citoyens envers le dispositif.

[8] Les UX designer appliquent une approche centrée sur les usagers afin d'améliorer leur expérience, de la simplifier et de la rendre utile.
[9] Les données y sont chiffrées avec des clés spécifiques à l'application via un mécanisme fourni par Android et iOS.
[10] Notamment l'article L. 300-2 du code des relations entre le public et l'administration.
[11] Circulaire n 6264/SG du 27 avril 2021 relative à la politique publique de la donnée, des algorithmes et des codes sources.

- La sécurité

Le dispositif apporte la garantie de l'Etat aux données d'identité des usagers transmises et vise le niveau de garantie élevé du règlement eIDAS. Le moyen d'identification électronique régalien fera, en conséquence, l'objet :

- d'une homologation selon le référentiel général de sécurité (RGS) par l'autorité d'homologation du ministère de l'intérieur ;
- d'une certification de sécurité de premier niveau (CSPN) par l'Autorité nationale de sécurité des systèmes d'information (ANSSI) pour chaque application mobile (Android et iOS) ;
- d'une qualification élémentaire par l'ANSSI pour répondre aux différents niveaux de garantie prévus par le règlement eIDAS.

F. Les usages du moyen d'identification électronique

Le moyen d'identification électronique proposé par l'Etat permettra aux usagers la réalisation de multiples usages :

- s'authentifier auprès de fournisseurs de téléservices publics ou privés tels notamment ceux accessibles via FranceConnect ;
- obtenir des attestations électroniques d'attributs d'identité, signées par l'Etat (cachet de l'État garantissant ainsi l'exactitude des données transmises), qui seront envoyées par les usagers aux tiers concernés pour transmettre leurs données d'identité dans le cadre de leurs démarches en ligne ;
- afficher sur l'écran de leur *ordiphone* la preuve de leur âge ou de leur majorité.

G. Le projet de développement

La mission impartie par les deux lettres de mission interministérielles des 5 janvier 2018 et 2 août 2019 correspond à la disposition du public, au cours du second semestre 2022, d'un moyen d'identification électronique sécurisé sur *ordiphone*, intégré à FranceConnect et qualifié par l'ANSSI au niveau de garantie substantiel au sens du règlement eIDAS, puis au niveau élevé. Ce moyen d'identification électronique sera, dans un premier temps, adossé aux cartes nationales d'identité disposant d'un composant électronique (été 2022), puis, dans un second temps, aux passeports biométriques et aux titres de séjour disposant d'un composant électronique (fin 2022).

Avant de parvenir à la qualification précitée par l'ANSSI, une étape intermédiaire est programmée, aux fins d'offrir des premiers usages numériques d'utilité immédiate. Ainsi, dès le premier trimestre 2022, une première application « compagnon » permettra aux usagers d'accéder aux données d'identité protégées dans le composant électronique de leur carte nationale d'identité et de bénéficier de deux premières fonctionnalités :

- l'obtention d'une attestation électronique d'attributs d'identité (ou d'un attribut d'identité), signée par l'Etat, pouvant être transmise par voie électronique[12] ;

[12] Cet usage répond notamment à la délibération du 11 février 2021 de la CNIL, qui « *encourage le développement de ces identités [identité numériques], sécurisées, qui permettent notamment de supprimer la circulation de photocopies de pièces d'Etat civil lors de l'accomplissement de certaines démarches administratives ou commerciales les nécessitant (…)* ».

- la possibilité d'afficher sur leur *ordiphone* la preuve de leur âge (en premier lieu celle de la majorité), facilitant l'accès à certains lieux réservés ou tarifs préférentiels par exemple, sans dévoiler l'ensemble des données présentes sur leur titre physique[13].

La responsabilité du traitement SGIN est exercée de façon conjointe 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 la tutelle du ministère de l'intérieur, conformément à l'article 26 du RGPD lorsque « deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement ».

L'ANTS est également le pouvoir adjudicateur qui porte la responsabilité de la passation et de l'exécution des marchés publics qui ont été conclus pour assurer la mise en œuvre du SGIN. L'ANTS, pour accomplir cette mission, fonctionne nécessairement en toute autonomie s'agissant du choix de ses sous-traitants et de la mobilisation de moyens financiers.

Afin de répondre aux exigences posées par le RGPD, et notamment son article 26 qui prévoit la signature d'un accord entre les différents responsables de traitement afin que soient définies de façon transparente leurs responsabilités respectives au regard du RGPD, une convention cadre entre l'ANTS et le ministère de l'intérieur sera établie au cours deuxième semestre 2022. Toute évolution concernant le statut des deux responsables de traitement identifiés *supra* pourra donner lieu à une actualisation de la présente AIPD.

[13] Cette possibilité répond également à une remarque de la CNIL, dans la délibération précitée, selon laquelle il « *est possible de prévoir des dispositifs d'identification procédant à la divulgation sélective des informations présentes sur la carte (fonctionnalité incluse dans la carte d'identité allemande). Cela pourrait permettre l'utilisation de la carte pour certaines finalités spécifiques sans avoir à révéler l'intégralité des données d'identité (par exemple pour certifier sa commune de résidence lorsque l'on souhaite bénéficier d'une réduction à l'entrée dans un équipement communal, sans révéler tous les éléments d'identité présents sur la carte ; ou pour certifier son âge pour jouer à un jeu d'argent ou acheter de l'alcool en donnant ces seuls éléments d'information)* ».

I. Vue d'ensemble fonctionnelle

Pour disposer d'un moyen d'identification électronique, les usagers doivent :

- être majeurs ;
- être titulaires d'une carte nationale d'identité disposant d'un composant électronique en cours de validité ;
- posséder un *ordiphone* disposant d'un système d'exploitation Android ou d'un système d'exploitation iOS et de la technologie sans contact (ou NFC), dans une version compatible c'est-à-dire une version contenant les mécanismes de sécurité suffisants.

La mise à disposition du public du moyen d'identification électronique repose sur trois macro processus :

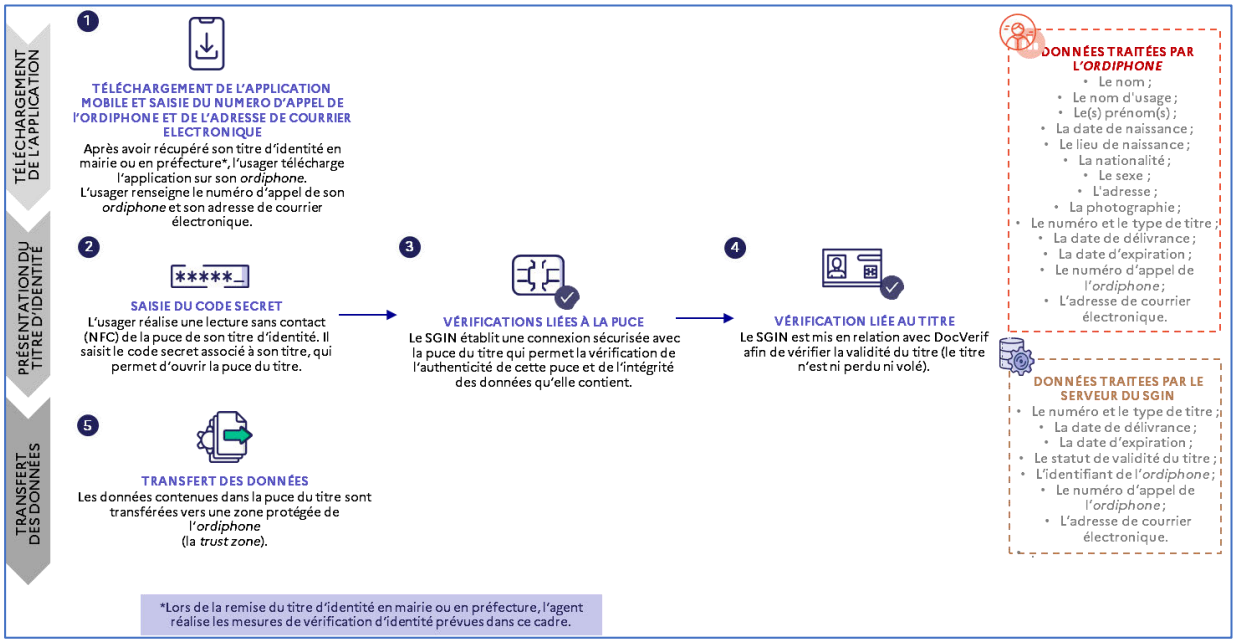
- sa délivrance ;
- son utilisation ;
- sa gestion.

A. La délivrance du moyen d'identification électronique

La délivrance du moyen d'identification électronique nécessite :

- un *ordiphone* dans une version compatible avec un lecteur NFC ;
- un titre d'identité en cours de validité ;
- le code secret associé au titre d'identité.

Schéma général



Processus détaillé

Description du processus	Données traitées[14]
Remise du titre en mairie ou en préfecture par un agent, après réalisation des mesures de vérification d'identité prévues dans ce cadre[15].	Le nom Le nom d'usage Le(s) prénom(s) La date de naissance Le lieu de naissance La nationalité Le sexe L'adresse postale extraite du titre La photographie extraite du composant électronique du titre Le numéro et le type de titre Sa date de délivrance Sa date d'expiration L'identifiant de l'*ordiphone*[16] Le numéro d'appel de l'*ordiphone*[17] L'adresse de courrier électronique[18] Le statut de validité du titre (valide/invalide/inconnu)
Téléchargement de l'application par l'usager sur son *ordiphone*.	
Lecture NFC du composant électronique du titre d'identité. Saisie de son code secret[19] par l'usager. Ce code est un facteur d'authentification. Il permet d'ouvrir le composant électronique du titre.	
Vérification de l'authenticité du composant électronique du titre d'identité[20] et de l'intégrité des données contenues dans ce composant électronique[21].	
Vérification de la validité du titre d'identité[22].	
Transfert des données contenues dans le composant électronique du titre d'identité vers une zone protégée de l'*ordiphone* (la « trust zone »).	

[14] A l'exception de l'identifiant de l'*ordiphone,* du numéro d'appel de l'*ordiphone,* de l'adresse de courrier électronique et du statut de validité du titre, les données mentionnées sont extraites du composant électronique du titre d'identité.

[15] Pour mémoire, lors de la remise du titre d'identité, l'usager est invité, par l'agent public, à présenter ses empreintes digitales sur un dispositif dédié pour vérifier qu'il en est bien le demandeur du titre concerné. Par ailleurs, l'agent public s'assure que le visage de l'usager correspond à celui-ci de la photographie du titre.

[16] Cette donnée est générée par le traitement.

[17] Cette donnée est renseignée par l'usager lors de la création du moyen d'identification électronique.

[18] Cette donnée est renseignée par l'usager lors de la création du moyen d'identification électronique.

[19] Ce code sera récupéré par l'usager dans un premier temps, uniquement à sa demande selon le même processus que pour la perte ou l'oubli (voir § C2), dans un deuxième temps de façon systématique. Dans les deux cas, une vérification d'identité sera opérée, soit par la remise d'un courrier expert, soit par la remise de l'attestation de remise du titre en mairie ou en préfecture qui le mentionnera de manière offusquée.

[20] La vérification de l'authenticité du composant électronique du titre d'identité consiste en la vérification du fait que le composant électronique est authentique, qu'il n'est pas un clone et qu'il a été personnalisé par l'Etat.

[21] La mémoire du composant électronique est structurée en groupes de données (DG, *data group*). Chaque data group utilisé est haché puis signé numériquement. Le résultat est stocké dans le SOD (objet de sécurité du document).
Le lecteur contrôle l'authenticité des data group contenus dans la mémoire du composant électronique en vérifiant que la signature de ces données est correcte. Il s'agit de vérifier que les données signées dans le titre (SOD) sont signées par une autorité de certification de l'Etat.

[22] Le SGIN est mis en relation avec DOCVERIF, qui transmet une information relative à la validité ou à l'absence de validité du titre d'identité (voir page 21 de l'AIPD).

B. L'utilisation du moyen d'identification électronique

Le moyen d'identification électronique sert à s'authentifier auprès de fournisseurs de services publics ou privés pour bénéficier de leurs services en ligne. Il sert également à l'obtention d'attestations électroniques d'attributs d'identité signées par l'Etat. Il sert enfin à apporter la preuve de l'âge ou de la majorité.

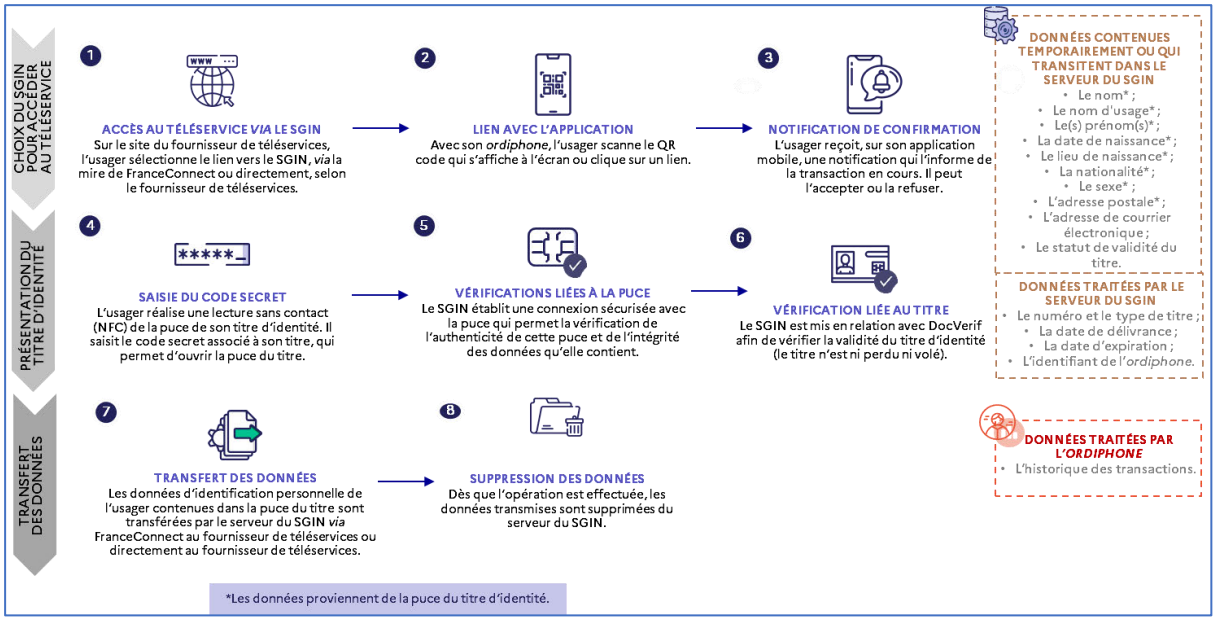
1. Les authentifications permettant l'accès à des téléservices publics ou privés

a. Les authentifications permettant l'accès à des téléservices exigeant un niveau de garantie élevé

Les authentifications permettent l'accès à des téléservices exigeant un niveau de garantie élevé permettent également l'accès aux services en ligne exigeant un niveau de garantie substantiel ou un niveau de garantie faible. Ces authentifications nécessitent :

- la présentation, par les usagers, de leur titre d'identité devant leur *ordiphone* pour une lecture NFC de ce titre ;
- la saisie de leur code secret.

Schéma général



Processus détaillé

Description du processus	Données traitées
Sur le site du fournisseur de téléservices, sélection du lien vers FranceConnect et sélection, dans la mire de FranceConnect, du SGIN. ou Hors FranceConnect, sur le site du fournisseur de téléservices, sélection du lien vers le SGIN.	Le nom Le nom d'usage Le(s) prénom(s) La date de naissance Le lieu de naissance La nationalité Le sexe L'adresse postale L'adresse de courrier électronique L'historique des transactions[23] L'identifiant de l'*ordiphone* Le numéro de titre Sa date de délivrance Sa date d'expiration Le statut de validité du titre (valide/invalide/inconnu)
Scan par l'usager *via* son *ordiphone* d'un QR code ou clic sur un lien pour ouvrir l'application mobile[24]. Réception, sur son application mobile, d'une notification informant l'usager de la transaction en cours qu'il peut accepter ou refuser.	
Lecture NFC du composant électronique du titre d'identité. Saisie de son code secret par l'usager.	
Vérification de l'authenticité du composant électronique du titre d'identité et de l'intégrité des données contenues dans ce composant électronique.	
Vérification de la validité du titre d'identité.	
Transfert des données d'identification personnelle de l'usager contenues dans le composant électronique du titre d'identité, par le serveur *via* FranceConnect au fournisseur de services ou directement au fournisseur de téléservices. Suppression du serveur des données transmises sitôt l'opération effectuée.	

b. Les authentifications permettant l'accès à des téléservices exigeant un niveau de garantie substantiel ou faible

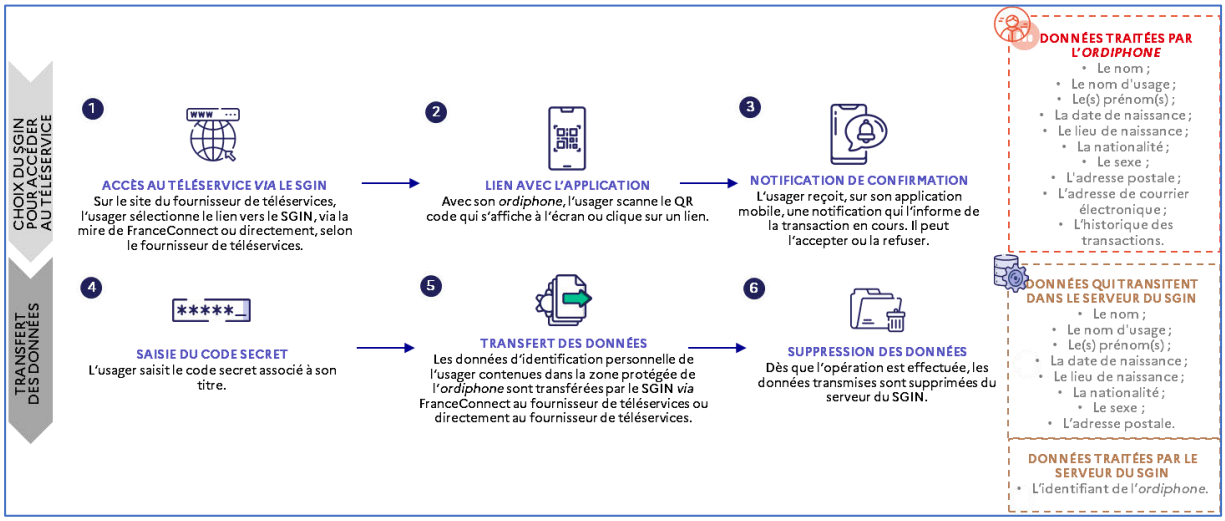
Le processus relatif aux authentifications permettant l'accès à des services exigeant un niveau de garantie substantiel ou faible est identique à celui qui permet l'accès à des services exigeant un niveau de garantie élevé, à l'exception de la présentation du titre et de la vérification de sa validité.

Les données d'identification personnelle transférées proviennent de la zone protégée ou trust zone, de l'*ordiphone* de l'usager.

[23] Cette donnée est générée par l'application mobile. Elle est conservée dans l'*ordiphone*.

[24] Le format du QR code et les principes de sécurité associés sont détaillés dans le tableau du chapitre "Description des mesures générales de sécurité »

Schéma général

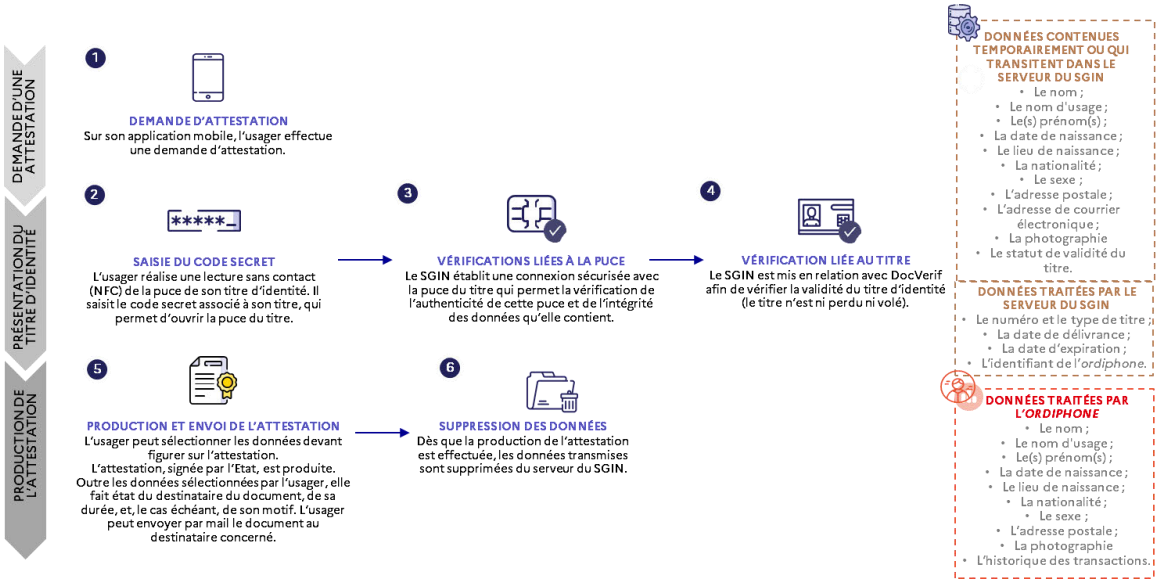


2. Les authentifications permettant l'obtention d'attestations électroniques d'attributs d'identité ou d'un attribut d'identité

Dans le cadre de leurs démarches administratives ou de leurs démarches privées, par exemple lorsqu'il est demandé d'attester de son identité auprès d'administrations, notamment les collectivités locales, ou pour souscrire une assurance, acquérir un bien immobilier, louer ou acheter un véhicule, etc., les usagers peuvent s'authentifier pour obtenir une attestation électronique d'attributs d'identité ou d'un attribut d'identité.

Les usagers ont la faculté d'indiquer le destinataire, le motif et la durée de validité de cette attestation, aux fins d'éviter de potentiels mésusages.

Schéma général



Processus détaillé

Description du processus	Données traitées
Lecture NFC du composant électronique du titre d'identité. Saisie de son code secret par l'usager.	Le nom Le nom d'usage Le(s) prénom(s) La date de naissance Le lieu de naissance La nationalité Le sexe L'adresse postale La photographie extraite du composant électronique du titre L'adresse de courrier électronique L'historique des transactions L'identifiant de l'*ordiphone* Le numéro de titre Sa date de délivrance Sa date d'expiration Le statut de validité du titre (valide/invalide/inconnu)
Vérification de l'authenticité du composant électronique du titre d'identité et de l'intégrité des données contenues dans ce composant électronique.	
Vérification de la validité du titre d'identité.	
Sélection, le cas échéant, par l'usager des données d'identité devant figurer sur le document électronique	
Obtention de l'attestation électronique d'attributs d'identité, signé par l'Etat[25], faisant état du destinataire du document, de sa durée, et le cas échéant, de son motif. Suppression du serveur des données utilisées pour obtenir le document électronique sitôt l'opération effectuée.	
Envoi par voie électronique du document par l'usager au destinataire concerné	

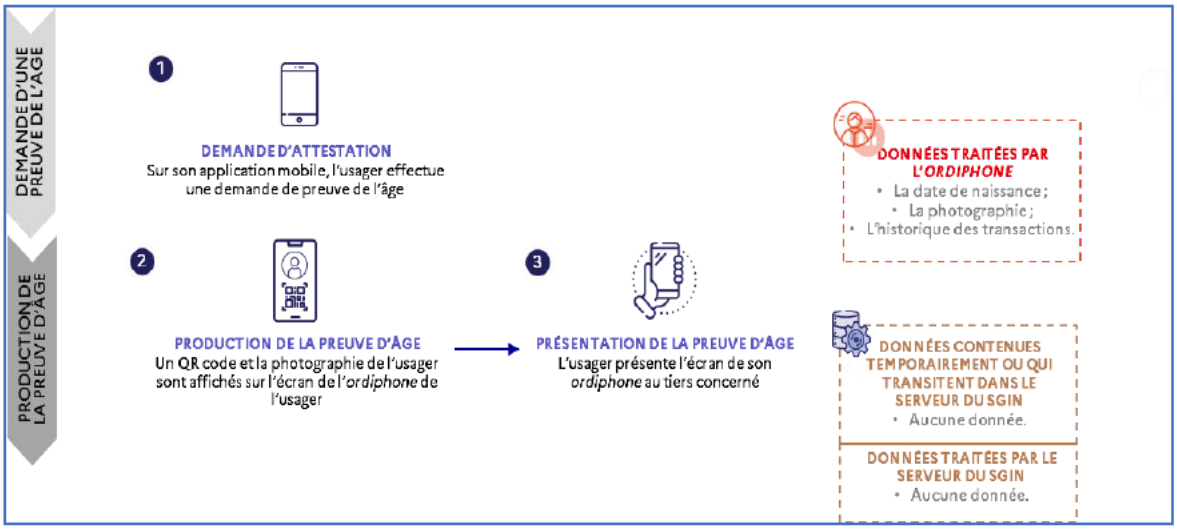
3. La preuve de l'âge ou de la majorité

Les usagers peuvent apporter la preuve de leur âge sur leur téléphone mobile, afin de bénéficier de tarifs préférentiels par exemple. Le cas d'usage prioritairement visé est l'affichage de la preuve de la majorité (sans préciser l'âge exact), afin de pouvoir accéder à certains services tels que l'accès aux discothèques, l'achat d'alcool, etc.

S'agissant de cet usage qui doit rester à la seule main des usagers, le serveur du SGIN n'est pas sollicité et le dispositif reste entièrement local.

[25] La signature par l'Etat de l'attestation électronique est systématique. Le document électronique est signé par l'Etat par la solution « cachet serveur ». La notion de signature « cachet serveur » implique que les clefs de signature sont situées sur le serveur (protégées dans un boitier cryptographique / HSM ou boîte noire transactionnelle) et non dans le titre d'identité. Les clefs de signature ne sont donc ni nominatives ni rattachées à un titre spécifique.

Schéma général



Processus détaillé

Description du processus	Données traitées
Saisie de son code secret par l'usager.	La date de naissance La photographie extraite du composant électronique du titre L'historique des transactions
Sélection par l'usager de la donnée à présenter (âge ou majorité).	
Affichage d'un QR code[26] et de la photographie[27] de l'usager sur l'écran de son *ordiphone*.	
Présentation de l'écran de son *ordiphone,* par l'usager, au tiers concerné.	

Le SGIN fournit, au travers de son application mobile, le moyen de scanner le QR code et de le vérifier au moyen de l'appareil photographique de l'*ordiphone*[28]. Aucune donnée n'est conservée, ni par le destinataire, ni dans l'application de l'usager.

C. Le processus de gestion du moyen d'identification électronique

1. Perte ou blocage du code secret

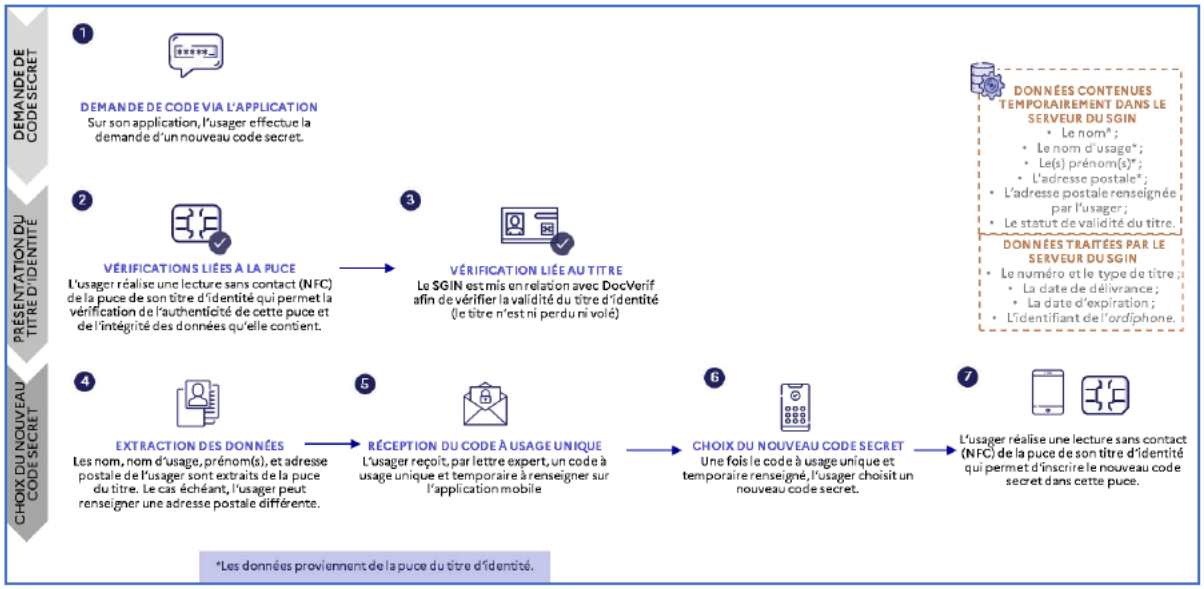
Le code secret se bloque dans l'hypothèse où l'usager réalise trois tentatives erronées de saisie.

[26] Le QR code s'appuie sur le standard 2D-DOC qui inclut une signature électronique.

[27] Comme vu *supra*, la photographie est extraite du composant électronique du titre d'identité lors de la délivrance du moyen d'identification électronique. Elle est conservée dans une zone protégée du téléphone portable. Lorsque les usagers souhaitent apporter la preuve de leur âge ou de leur majorité, cette donnée s'affiche, après authentification réussie, sur l'écran de leur *ordiphone*. Elle provient de cette zone protégée.

[28] Comme il est actuellement effectué par TousAntiCovid Verif.

Schéma général



Processus détaillé

Description du processus	Données traitées
Demande sur l'application d'un nouveau code secret	Le nom Le nom d'usage Le(s) prénom(s) L'adresse postale extraite du titre ou, le cas échéant, l'adresse postale renseignée par l'usager Le numéro et le type de titre Sa date de délivrance Sa date d'expiration L'identifiant de l'*ordiphone*
Lecture NFC du composant électronique du titre d'identité. Vérification de l'authenticité du composant électronique du titre d'identité et de l'intégrité des données contenues dans ce composant électronique.	
Vérification de la validité du titre d'identité.	
Extraction du composant électronique du titre d'identité des nom, nom d'usage, prénom(s) et adresse postale de l'usager. Le cas échéant, l'usager peut renseigner une adresse postale différente.	
Réception par lettre expert[29] d'un code à usage unique et temporaire à renseigner sur l'application mobile.	
Lecture du titre et choix d'un nouveau code secret[30].	

[29] Une lettre expert est un courrier remis en main propre de l'usager après vérification de son identité par le facteur.

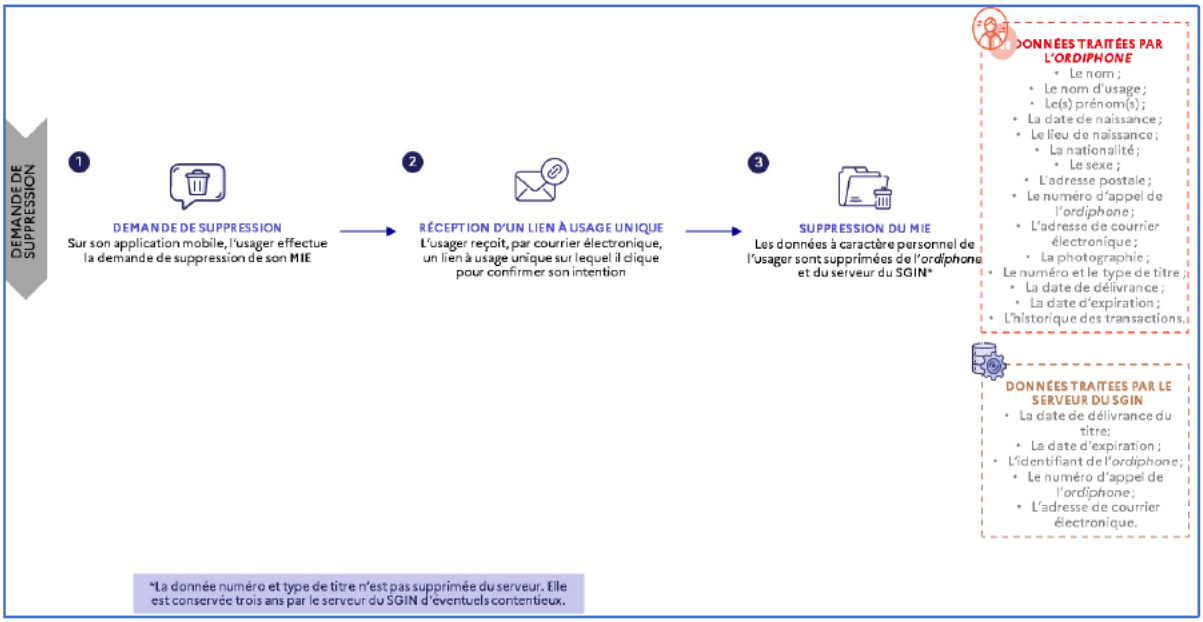
[30] Le choix du code secret doit obéir aux principes suivants :
- les motifs de deux ou trois chiffres (exemple : 119117, 123123) ou les suites de quatre chiffres (exemple : 0123, 1234, 4567) sont interdits ;
- le code secret doit contenir au moins trois chiffres différents ;
- le code secret doit être différent de la date de naissance de l'usager (au format JJMMAA).

Description du processus	Données traitées
	Le statut de validité du titre

2. Suppression du moyen d'identification électronique par les usagers *via* l'application mobile

L'usager peut à tout moment supprimer son moyen d'identification électronique *via* l'application mobile sur son *ordiphone*.

Schéma général



Processus détaillé

Description du processus	Données traitées
Demande de suppression sur l'application mobile	Le nom Le nom d'usage Le(s) prénom(s) La date de naissance Le lieu de naissance La nationalité Le sexe L'adresse postale
Réception par l'usager d'un lien à usage unique, par courrier électronique, sur lequel il doit cliquer pour confirmer son intention.	
Suppression des données à caractère personnel de l'*ordiphone* et du serveur[31].	

[31] La donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour le traitement d'éventuels contentieux.

Description du processus	Données traitées
	La photographie extraite du composant électronique du titre La date de délivrance La date d'expiration L'historique des transactions L'identifiant de l'*ordiphone* Le numéro d'appel de l'o*rdiphone* L'adresse de courrier électronique

3. La révocation du moyen d'identification électronique

En cas de perte ou de vol de son *ordiphone*[32], l'usager peut révoquer son moyen d'identification électronique.

Schéma général

Processus détaillé

Description du processus	Données traitées
Sur le site web du SGIN, saisie de l'adresse de courrier électronique de l'usager ou de son numéro d'appel d'*ordiphone*	Le numéro d'appel d'*ordiphone* L'adresse de courrier électronique
Réception d'un code à usage unique par courrier électronique ou SMS	
Saisie du code à usage unique sur le site web du SGIN	
Révocation du moyen d'identification électronique dans le SGIN.	

[32] La déclaration sur DOCVERIF de la perte ou du vol du titre d'identité permet de rendre inutilisable ce titre et donc l'utilisation du moyen d'identification électronique en mode élevé. En revanche, le moyen d'identification électronique reste, dans cette hypothèse, utilisable en mode substantiel ou faible.

Description du processus	Données traitées
Les données à caractère personnel des usagers ne sont pas supprimées.	

D. Les interfaces

La délivrance et la création du moyen d'identification électronique nécessitent des interfaces avec :

1. DOCVERIF

Le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015[33] impose, pour la délivrance des moyens d'identification électronique de niveau de garantie substantiel, que des mesures aient été prises pour minimiser le risque que l'identité de la personne ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification.

Dans ce cadre et afin d'ajouter des sécurités supplémentaires lors de l'utilisation du moyen d'identification électronique, une interconnexion est prévue avec le fichier national de contrôle de la validité des titres (DOCVERIF)[34]. Celle-ci permet de garantir que le titre d'identité utilisé est valide c'est-à-dire qu'il n'est ni perdu, ni volé, ni inconnu, dans les hypothèses suivantes :

- les usagers créent un moyen d'identification électronique,
- ils s'authentifient pour accéder à des services exigeant un niveau de garantie élevé,
- ils s'authentifient pour obtenir des attestations électroniques d'attributs d'identité ou d'un attribut d'identité.

L'interrogation de DOCVERIF implique :

- le numéro du titre ;
- le type du titre ;
- sa date de délivrance.

Elle retourne le statut de validité administrative du titre :

- valide : le titre est administrativement valide ;
- invalide : le titre est perdu, volé ou invalidé pour une autre raison ;
- inconnu : la combinaison numéro, type et date de délivrance du titre n'existe pas dans le référentiel du service DOCVERIF.

En cas d'invalidité du titre d'identité, le SGIN n'a jamais connaissance du motif précis (perdu ou volé). Il a simplement connaissance du fait que le titre est invalide.

La donnée relative à la validité ou l'absence de validité du titre est supprimée du serveur du SGIN sitôt la vérification effectuée.

[33] Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement eIDAS.
[34] Arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF ».

2. Le système d'information d'un opérateur postal

L'interface avec le système d'information d'un opérateur postal permet au traitement l'envoi d'un code à usage unique, par le biais d'une lettre expert, pour permettre à l'usager de définir un code secret ou

Ainsi, lorsque l'usager sollicite l'envoi d'un code de déblocage au travers de l'application mobile le service central génère un code à usage unique, met en forme le courrier et transmet les données nécessaires à l'acheminement du courrier suivi à l'usager à l'opérateur postal :

- le courrier sous format électronique ;
- la civilité, les noms et prénoms de l'usager ;
- son adresse postale, éventuellement corrigée via le parcours de demande de déblocage.

L'impression, l'acheminement et la remise avec vérification de l'identité à l'usager sont gérées par l'opérateur postal.

3. FranceConnect

L'interface avec FranceConnect permet aux usagers de s'authentifier pour accéder à des services en ligne proposés par des fournisseurs de services, partenaires.

FranceConnect transmet aux fournisseurs de services concernés les données d'identification personnelle des usagers.

Les fournisseurs de services concernés sont :

- les autorités administratives partenaires habilitées à traiter les démarches et formalités des usagers en vertu d'un texte législatif ou réglementaire ;
- les personnes morales mentionnées au II et au III de l'article 1er de l'ordonnance n° 2005-395 du 28 avril 2005 relative au service public du changement d'adresse qui proposent des services en ligne liés à la démarche de changement d'adresse et uniquement pour ces services ;
- les personnes morales de droit privé qui proposent des services en ligne dont l'usage nécessite, conformément à des dispositions législatives ou règlementaires, la vérification de l'identité de leurs utilisateurs ou de celle de certains de leurs attributs et uniquement pour les services qui nécessitent cette vérification.

L'interface entre le service central du SGIN et FranceConnect s'appuie sur le protocole standard OpenID Connect[35] de façon à supporter :

- l'authentification d'un usager ;
- son consentement à transmettre les attributs d'identités demandés par le fournisseur de service partenaire ;
- sa déconnexion du service.

Dans le cadre du SGIN, sont transmises lors de la connexion à FranceConnect les données d'identité pivot de l'usager (son nom, son nom d'usage, son(ses) prénom(s), sa date de naissance, son lieu de naissance, son sexe), ainsi que son adresse de messagerie de contact.

[35] L'interface FranceConnect pour les fournisseurs d'identité est disponible sur https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-identite

4. Les fournisseurs de services qui ne sont pas interfacés avec FranceConnect

Cette interface permet aux usagers de s'authentifier pour accéder aux services en ligne de fournisseurs de services partenaires des responsables du traitement.

Le traitement transfère directement à ces fournisseurs les données d'identification personnelles des usagers concernés.

Comme dans le cadre d'une authentification FranceConnect, l'interface de connexion du SGIN avec les fournisseurs de services non interfacés avec FranceConnect s'appuie sur le protocole OpenID Connect de façon à permettre à l'usager :

- de s'authentifier ;
- de consentir à la transmission de certaines de ses données personnelles ;
- de se déconnecter du service.

A la différence de FranceConnect, la transmission de l'ensemble des attributs formant l'identité pivot n'est pas obligatoire, seuls les attributs demandés par le fournisseur sont transmis[36]. Les attributs souhaités par le fournisseur de services sont demandés au travers du protocole OpenID Connect, notifiés à l'usager avant la saisie du code secret puis transmis directement du fournisseur de services au travers du serveur.

5. Services de la direction du numérique du ministère de l'intérieur

Le serveur du SGIN est interfacé avec plusieurs services de la direction du numérique du ministère de l'intérieur :

- le service de signature électronique, utilisé dans le cadre de la signature « cachet serveur » des attestations électroniques d'attributs d'identité. Il est accessible au travers d'une API avec authentification mutuelle ;
- le service d'horodatage qualifié eIDAS, utilisé dans le cadre de la signature « cachet serveur » des attestations électroniques d'attributs d'identité, afin d'y insérer une date de confiance, et pour sécuriser les journaux d'événements du service central. Le service d'horodatage est accessible au travers d'une API avec authentification mutuelle ;
- le service de relai de messagerie électronique, qui s'appuie sur le protocole SMTP avec STARTTLS pour l'envoi de courriers électroniques aux usagers.

6. Service d'envoi de SMS

Le service d'envoi de SMS du marché « SMS en masse » du ministère de l'intérieur, accessible sur internet depuis une API, permet l'envoi de codes à usage unique aux usagers dans le cadre de la révocation de l'identité numérique.

L'API requiert deux paramètres :

- L'adresse de destination : le numéro de téléphone précédé du code pays (exemple : « 33123456789 ») ;
- Le contenu du message (exemple : « Votre code temporaire SGIN est 1234 »).

[36] Ces données peuvent être le nom, le nom d'usage, le(s) prénom(s), la date de naissance, le lieu de naissance, la nationalité, le sexe, l'adresse postale extraite du composant électronique du titre d'identité, et l'adresse de courrier électronique.

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

1. Les accédants

Peuvent accéder aux données à caractère personnel des usagers :

- Les agents des services du secrétariat général (Programme interministériel France identité numérique) et les agents de l'Agence nationale des titres sécurisés, chargés de la maîtrise d'ouvrage et de la maîtrise d'œuvre du traitement. Ces agents sont individuellement désignés et spécialement habilités par leur directeur.

  Dans le cadre de leurs missions, les agents des services des responsables du traitement peuvent donc accéder aux données à caractère personnel des usagers qui sont conservées sur le serveur du SGIN, soit leur numéro de téléphone portable, leur adresse de courrier électronique, l'identifiant de leur *ordiphone*, leur numéro de titre, la date de délivrance de ce titre et sa date d'expiration.

  Sur demande des autorités judiciaires ou des personnes concernées, ces agents peuvent également avoir accès aux traces d'utilisation du MIE.

- Les usagers eux-mêmes lorsqu'ils obtiennent des attestations électroniques d'attributs d'identité.

  Les données concernées peuvent être leur nom, leur nom d'usage, leur(s) prénom(s), leur date de naissance, leur lieu de naissance, leur nationalité, leur sexe, l'adresse postale extraite du composant électronique de leur titre d'identité, la photographie extraite du composant électronique de leur titre d'identité et leur adresse de courrier électronique.

  Les usagers sélectionnent les données qu'ils souhaitent voir figurer sur leurs attestations électroniques d'attributs d'identité.

  Les usagers transmettent ces attestations aux personnes physiques ou morales de leur choix.

2. Les destinataires

Peuvent recevoir les données à caractère personnel des usagers :

- Le téléservice FranceConnect ;
- Les fournisseurs de téléservices liés par convention à FranceConnect, auxquels FranceConnect transmet les données sans modification ;
- Les fournisseurs de téléservices liés par convention aux responsables du traitement ;
- Les personnes physiques ou morales auxquelles les usagers souhaitent transmettre une attestation électronique d'attributs d'identité.

Les données concernées peuvent être le nom, le nom d'usage, le(s) prénom(s), la date de naissance, le lieu de naissance, la nationalité, le sexe, l'adresse postale extraite du composant électronique de leur titre d'identité, le cas échéant, la photographie extraite du composant électronique du titre d'identité et l'adresse de courrier électronique.

II. Vue d'ensemble juridique

1. Quelles sont les responsabilités liées au traitement ?

Les responsables de traitement sont le secrétaire général du ministère de l'intérieur et l'agence nationale des titres sécurisés.

Le responsable du traitement est à la fois maîtrise d'ouvrage et maîtrise d'œuvre du traitement.

Le responsable du traitement fait appel à des sous-traitants, maîtrises d'œuvre du traitement.

2. Quels sont les référentiels applicables ?

- Le règlement eIDAS, qui a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur en établissant un cadre d'interopérabilité, donne une définition de l'identification électronique[37] ainsi que des moyens utilisés pour réaliser cette identification électronique[38] et établit trois niveaux de garantie (faible, substantiel, élevé) pour ces moyens d'identification électronique ;
- L'article L. 102 du code des postes et des communications électroniques traite spécifiquement des moyens d'identification électronique en prévoyant qu'ils puissent faire l'objet d'une certification par l'Etat et en créant une présomption de fiabilité lorsque ceux-ci répondent aux prescriptions du cahier des charges qui doit être établi par l'ANSSI et fixé par décret en Conseil d'Etat. Ce décret est en cours de rédaction ;
- Le règlement sur la carte nationale d'identité[39] impose aux Etats-membres de délivrer, à compter du mois d'août 2021, une carte nationale d'identité disposant d'un composant électronique comprenant des données alphanumériques et des données biométriques de son titulaire (photographie et empreintes digitales) dont l'objet premier est la libre circulation mais dont il est expressément indiqué (considérant 15) qu'elle peut contribuer à l'identification électronique ;
- La loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité définit, dans son article 2, les données contenues dans le composant électronique de la carte d'identité et dispose, dans son article 6, que l'identité du possesseur de cette carte nationale est justifiée à partir des données inscrites sur le document lui-même ou dans le composant électronique sécurisé ;
- Le règlement général sur la protection des données (ou RGPD)[40] pose un nouveau cadre juridique en matière de protection des données personnelles des citoyens européens afin de répondre aux évolutions du numérique ;
- La loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

[37] Selon le 2. de l'article 3 du règlement eIDAS, l'identification électronique désigne le « *processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* ».
[38] Selon le 1. de l'article 3 du règlement eIDAS, le moyen d'identification électronique désigne « *un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne* ».
[39] Règlement (UE) 2019/1157 du Parlement européen et du conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation.
[40] 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).

- Le code des relations entre le public et l'administration, et notamment son article R. 112-9-1 ;
- Le décret n° 55-1397 du 22 octobre 1955 modifié instituant la carte nationale d'identité ;
- Le décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité ;
- L'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;
- L'arrêté du 20 septembre 2019 portant référentiel général d'amélioration de l'accessibilité.

3. Les finalités du traitement sont-elles déterminées, explicites et légitimes ?

La finalité du traitement est déterminée : proposer aux titulaires d'une carte nationale d'identité comportant un composant électronique, tel que mentionné à l'article 1-1 du décret du 22 octobre 1955, la délivrance d'un moyen d'identification électronique leur permettant de s'identifier et de s'authentifier électroniquement auprès d'organismes publics ou privés, au moyen d'un *ordiphone* doté d'un dispositif permettant la lecture sans contact du composant électronique de ce titre.

La finalité du traitement est légitime au regard des services rendus aux usagers ainsi qu'aux tiers :

- Délivrance, dans des conditions sécurisées, d'un moyen d'identification électronique :

  Avec le moyen d'identification électronique proposé par l'Etat, les usagers ont la totale maîtrise de leurs données d'identité, uniquement conservées dans le composant électronique de leur titre d'identité et dans une zone protégée de leur *ordiphone.* Si ces données transitent par le serveur du SGIN pour les besoins de leur authentification, elles en sont supprimées sitôt leur communication aux tiers concernés réalisée.

  Les données à caractère personnel sont effacées de l'*ordiphone* des usagers et du serveur du SGIN[41] si ces derniers suppriment leur moyen d'identification électronique *via* l'application mobile
- Réduction du risque d'usurpation d'identité grâce à un processus d'authentification sécurisé ;
- Contribution à la dématérialisation des démarches y compris les plus sensibles.

Quel(s) est (sont) les fondement(s) qui rend(ent) votre traitement licite ?

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 les responsables du traitement conformément aux dispositions du e) de l'article 6-1. du règlement général sur la protection des données.

La délivrance des titres d'identité aux citoyens relève de la compétence exclusive de l'Etat. Cette mission régalienne est essentielle : elle garantit l'identité des personnes concernées et elle leur permet de prouver leur identité, leur nationalité et d'exercer leur citoyenneté.

[41] La donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour le traitement d'éventuels contentieux.

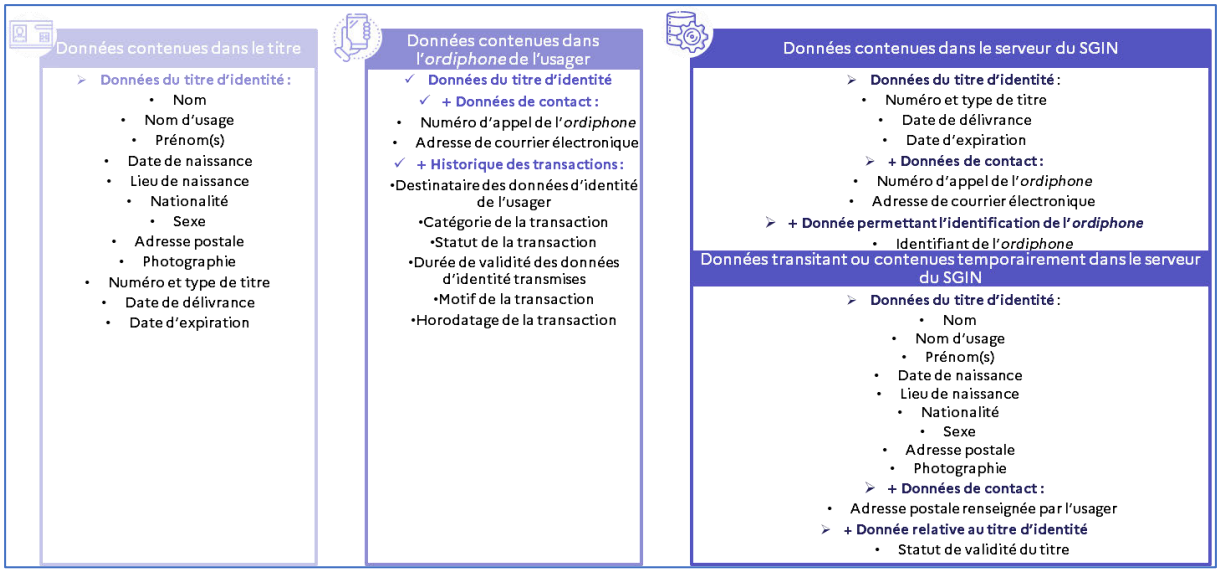
En proposant un moyen d'identification électronique sécurisé, gratuit et inclusif, adossé à la carte nationale d'identité comprenant un composant électronique, l'Etat permet aux citoyens de prouver leur identité en ligne comme ils le font dans le monde physique.

Ce faisant, il permet la mise en œuvre d'une solution de dématérialisation intégrale de leurs démarches. Le déploiement de ce service sécurisé contribuera à la confiance dans l'écosystème numérique.

L'Etat a également pour mission de lutter contre l'usurpation d'identité. Le moyen d'identification électronique régalien, qui vise les niveaux de garantie élevé et substantiel au sens du règlement eIDAS, a pour objectif de contribuer à la lutte contre l'usurpation d'identité en ligne en garantissant aux usagers, aux organismes privés et publics ainsi qu'aux tiers l'identité des personnes concernées.

A. Quelles sont les données à caractère personnel traitées, où sont-elles conservées et combien de temps ?

Le détail des données traitées est le suivant :



Les données à caractère personnel concernées par le traitement peuvent être conservées dans la zone protégée de l'*ordiphone* après chiffrement, et/ou sur le serveur du SGIN.

La zone protégée ou trust zone est une zone physique de l'*ordiphone*. Les données qui y sont conservées sont chiffrées avec des clés spécifiques à l'application via un mécanisme fourni par Android et iOS.

1. Les données à caractère personnel traitées par l'*ordiphone*

Catégorie de données	Données	Rôle	Origine	Durée de conservation
Données du titre d'identité	Nom	Données nécessaires aux authentifications des usagers	Extraction du composant électronique du titre d'identité	Cinq ans maximum (durée de validité de l'identité numérique selon le référentiel général de sécurité (RGS))
	Nom d'usage			
	Prénom(s)			
	Date de naissance			
	Lieu de naissance			
	Nationalité			
	Sexe			
	Adresse postale			
	Photographie	Données nécessaires aux authentifications des usagers		
	Numéro et type de titre	Donnée transmise au serveur du SGIN pour la réalisation des authentifications du titre d'identité Donnée transmise au serveur du SGIN pour l'interrogation de DOCVERIF Donnée transmise au serveur du SGIN pour retrouver les opérations de création, de consultation, d'utilisation, de révocation et de suppression du moyen d'identification électronique en cas de contentieux		
	Date de délivrance	Donnée transmise au serveur du SGIN pour l'interrogation de DOCVERIF		
	Date d'expiration	Donnée transmise au serveur du SGIN pour vérifier l'absence d'expiration du titre d'identité		
Données de contact	Le numéro d'appel de l'*ordiphone* si l'usager a renseigné cette donnée	Données nécessaires aux échanges avec les usagers et à la sécurisation des processus Données transmises au serveur du SGIN pour les échanges avec les usagers et la sécurisation des processus	Renseignement par les usagers	Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
	Adresse de courrier électronique			
Historique des transactions	Destinataire des données d'identification personnelle de l'usager	Données nécessaires à l'information des usager et à la sécurisation des processus	Générées automatiquement	
	Catégorie de la transaction			

	Statut de la transaction			(durée de validité de l'identité numérique selon le RGS)
	Durée de validité des données d'identification personnelle de l'usager transmises			
	Horodatage de la transaction			
	Motif de la transmission des données d'identification personnelle de l'usager			

2. Les données à caractère personnel traitées par le serveur du SGIN

Catégorie de données	Données	Rôle	Origine	Durée de conservation
Données du titre d'identité	Nom	Données nécessaires à l'identification des usagers auprès de tiers	Composant électronique du titre d'identité ou zone protégée de l'*ordiphone*	Suppression sitôt la transmission des données aux tiers concernés réalisées
		Données nécessaires dans l'hypothèse d'une demande d'un code secret par l'usager Données nécessaires dans l'hypothèse d'un changement de code secret en cas de blocage ou de perte	Composant électronique du titre d'identité	Suppression sitôt l'opération contribuant à l'obtention du code secret réalisée
	Nom d'usage	Données nécessaires à l'identification des usagers auprès de tiers	Composant électronique du titre d'identité ou zone protégée de l'*ordiphone*	Suppression sitôt la transmission des données aux tiers concernés réalisées
		Données nécessaires dans l'hypothèse d'une demande d'un code secret par l'usager Données nécessaires dans l'hypothèse d'un changement de code secret en cas de blocage ou de perte	Composant électronique du titre d'identité	Suppression sitôt l'opération contribuant à l'obtention du code secret réalisée
	Prénom(s)	Données nécessaires à l'identification des usagers auprès de tiers	Composant électronique du titre d'identité ou zone protégée de l'*ordiphone*	Suppression sitôt la transmission des données aux tiers concernés réalisées
		Données nécessaires dans l'hypothèse d'une demande d'un code secret par l'usager	Composant électronique du titre d'identité	Suppression sitôt l'opération contribuant à l'obtention du code secret réalisée

Catégorie de données	Données	Rôle	Origine	Durée de conservation
		Données nécessaires dans l'hypothèse d'un changement de code secret en cas de blocage ou de perte		

Catégorie de données	Données	Rôle	Origine	Durée de conservation
	Adresse postale	Données nécessaires à l'identification des usagers auprès de tiers	Composant électronique du titre d'identité ou zone protégée de l'*ordiphone*	Suppression sitôt la transmission des données aux tiers concernés réalisées

Catégorie de données	Données	Rôle	Origine	Durée de conservation
		Données nécessaires dans l'hypothèse d'une demande d'un code secret par l'usager Données nécessaires dans l'hypothèse d'un changement de code secret en cas de blocage ou de perte	Composant électronique du titre d'identité	Suppression sitôt l'opération contribuant à l'obtention du code secret réalisée
	Date de naissance Lieu de naissance Nationalité Sexe Photographie extraite du composant électronique du titre	Données nécessaires à l'identification des usagers auprès de tiers	Composant électronique du titre d'identité ou zone protégée de l'*ordiphone*	Suppression sitôt la transmission des données réalisées
	Numéro et type de titre	Donnée nécessaire à l'interrogation de DOCVERIF	*Ordiphone*	Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
		Donnée nécessaire à l'exercice des droits des personnes concernées		
		Donnée nécessaire pour faire face à d'éventuels contentieux		Trois ans
	Date de délivrance	Donnée nécessaire à l'interrogation de DOCVERIF		Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
	Date d'expiration	Donnée nécessaire à la vérification de l'absence d'expiration du titre d'identité		
Données de contact	Numéro d'appel de l'*ordiphone* si l'usager a renseigné cette donnée	Données nécessaires aux échanges avec les usagers et à la sécurisation des processus	*Ordiphone*	Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
	Adresse de courrier électronique	Données nécessaires à l'identification des usagers auprès de tiers		Suppression sitôt la transmission des données réalisées
		Données nécessaires aux échanges avec les usagers et à la sécurisation des processus		Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
	Adresse postale extraite du titre Le cas échéant, l'adresse postale renseignée par l'usager	Donnée nécessaire dans l'hypothèse d'une demande d'un code secret par l'usager Donnée nécessaire dans l'hypothèse d'un changement de code secret en cas de blocage ou de perte	Composant électronique du titre d'identité Renseignement par l'usager	Suppression sitôt l'opération contribuant à l'obtention du code secret réalisée

Catégorie de données	Données	Rôle	Origine	Durée de conservation
Donnée permettant l'identification de l'*ordiphone*	Identifiant de l'*ordiphone*	Donnée nécessaire à l'identification de l'*ordiphone*	*Ordiphone*	Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
Donnée relative au titre d'identité	Statut de validité du titre (valide/invalide/inconnu)	Donnée nécessaire pour savoir si le titre d'identité utilisé pour la délivrance et l'utilisation du moyen d'identification électronique est en cours de validité	DOCVERIF	Suppression sitôt la vérification effectuée

Si les usagers n'achèvent pas la délivrance du moyen d'identification électronique, les données à caractère personnel sont supprimées de l'*ordiphone* et du serveur du SGIN à l'issue d'un délai de deux mois[42].

Les données à caractère personnel sont supprimées de l'*ordiphone* et du serveur du SGIN[43] à l'issue d'une période d'inactivité de deux ans.

Les données à caractère personnel sont supprimées de l'*ordiphone* et du serveur du SGIN[44] lorsque les usagers :

- Suppriment le moyen d'identification électronique *via* l'application mobile.

B. Les données sont-elles exactes et tenues à jour ?

Lorsque les données à caractère personnel proviennent du composant électronique du titre d'identité, elles ne peuvent pas être modifiées par les usagers.

Les données de contact (numéro d'appel de *l'ordiphone* et adresse de courrier électronique) peuvent être modifiées par les usagers par une fonctionnalité prévue à cet effet.

Les données générées par l'application mobile et l'*ordiphone* (historique des transactions et identifiant de l'*ordiphone*) ne peuvent pas être modifiées par les usagers.

C. Les droits des personnes concernées

1. Comment les personnes concernées sont-elles informées à propos du traitement ?

Conformément aux exigences de l'article 13 du règlement général sur la protection des données, les personnes concernées sont informées des traitements effectués. Elles peuvent recueillir des informations précises sur le traitement sur :

- Le site de la direction du programme interministériel France identité numérique ;
- Le portail internet de l'ANTS ;
- La politique de sécurité et de confidentialité du traitement.

A titre individuel, une information est donnée lors de la délivrance du moyen d'identification électronique, *via* un lien hypertexte relatif au traitement des données à caractère personnel prévu à cet effet.

Conformément à l'article 13 du règlement général sur la protection des données, les précisions suivantes seront apportées aux usagers :

- Les identités des responsables de traitement et du délégué à la protection des données ;
- Les finalités et la base de licéité du traitement ;

[42] Ce délai de deux mois tient compte du délai de quinze jours permettant à l'usager d'aller récupérer la lettre expert contenant le code à usage unique chez l'opérateur postal et d'un délai d'un mois et demi laissé à l'usager pour saisir ce code à usage unique dans l'application mobile afin de définir un code secret.

[43] La donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour le traitement d'éventuels contentieux.

[44] La donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour le traitement d'éventuels contentieux.

- Les données à caractère personnel traitées, les lieux et leur durée de conservation ;
- Les destinataires des données à caractère personnel ;
- Les personnes habilitées à traiter les données à caractère personnel ;
- Les droits des personnes concernées ;
- Le droit d'introduire un recours devant la CNIL.

L'information se traduira également par des explications pédagogiques écrites et des vidéos adaptées à la compréhension de tous les publics susceptibles d'être concernés par le traitement.

2. Si applicable, comment le consentement des personnes concernées est-il obtenu ?

Le traitement n'a pas pour base de licéité le consentement. En revanche, la délivrance et l'utilisation du moyen d'identification résulte de la seule volonté des usagers. Comme indiqué précédemment, il s'agit d'un service optionnel, dont l'utilisation est à la discrétion des usagers.

3. Comment les personnes concernées peuvent-elles exercer leurs droit d'accès et droit à la portabilité ?

Le **droit d'accès** (cf. article 15 du RGPD) ne s'applique qu'aux données à caractère personnel conservées dans le serveur du SGIN (cf. paragraphe « quelles sont les données à caractère personnel traitées, où sont-elles conservées, combien de temps ? »).

Le droit d'accès s'exerce, auprès des responsables de traitement (la répartition des rôles entre eux sera abordée dans la convention prévue en page 11), par l'envoi d'un courrier électronique accompagné de la copie d'un titre d'identité (CNI/passeport) à l'adresse de courrier électronique suivante :

contact@france-identite.gouv.fr.

Le **droit à la portabilité** : non applicable au regard de la base de licéité du traitement (cf. 3. de l'article 20 du RGPD).

4. Comment les personnes concernées peuvent-elles exercer leur droit de rectification et leur droit à l'effacement (droit à l'oubli) ?

Le **droit à la rectification** s'applique aux seules données de contact conservées dans le serveur du SGIN (numéro d'appel de l'*ordiphone* et adresse de courrier électronique) dans la mesure où les autres données ont été extraites du titre d'identité, ont été générées par l'application mobile ou l'*ordiphone* ou en ont été supprimées (cf. paragraphe « quelles sont les données à caractère personnel traitées, où sont-elles conservées, combien de temps ? »).

Ce droit s'exerce, auprès des responsables de traitement (la répartition des rôles entre eux sera abordée dans la convention prévue en page 11), par l'envoi d'un courrier électronique accompagné de la copie d'un titre d'identité (CNI/passeport) à l'adresse de courrier électronique suivante :

contact@france-identite.gouv.fr.

Le **droit à l'effacement** : non applicable au regard de la base de licéité du traitement (cf. b) du 3 de l'article 17 du RGPD).

5. Comment les personnes concernées peuvent-elles exercer leurs droits à la limitation et leurs droits d'opposition ?

Le **droit à la limitation (cf. article 18 du RGPD) :** les usagers disposent du droit à la limitation du traitement. Toutefois, en pratique, ce droit ne pourra utilement être exercé dans la mesure où les identifications et les authentifications des usagers, exercées à leur seule initiative, requièrent la totalité de leurs données d'identité.

Ce droit s'exerce, auprès des responsables de traitement (la répartition des rôles entre eux sera abordée dans la convention prévue en page 11), par l'envoi d'un courrier électronique accompagné de la copie d'un titre d'identité (CNI/Passeport) à l'adresse de courrier électronique suivante :

contact@france-identite.gouv.fr.

Le **droit d'opposition :**

Le traitement repose entièrement sur un usage facultatif par les usagers. Compte tenu de ce principe du volontariat, le droit d'opposition s'exerce par la possibilité offerte à l'usager de supprimer leur moyen d'identification électronique ou de désinstaller l'application mobile de leur *ordiphone.* Leurs données à caractère personnel sont alors supprimées.

Les traces relatives aux opérations de création, consultation, utilisation, révocation et suppression du moyen d'identification électronique sont conservées trois ans pour faire face à un éventuel contentieux[45].

D. Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?

Les relations entre les responsables du traitement et ses sous-traitants sont régies par un contrat spécifique, conformément à l'article 28 du règlement général sur la protection des données.

Les sous-traitants sont Atos, Sopra Stéria, Idemia, Idakto et l'opérateur en charge de l'impression et de la mise sous pli des documents destinés à être envoyés par lettre expert aux usagers. Si des prestataires fournissent des captcha, ces fournisseurs seront également sous-traitants.

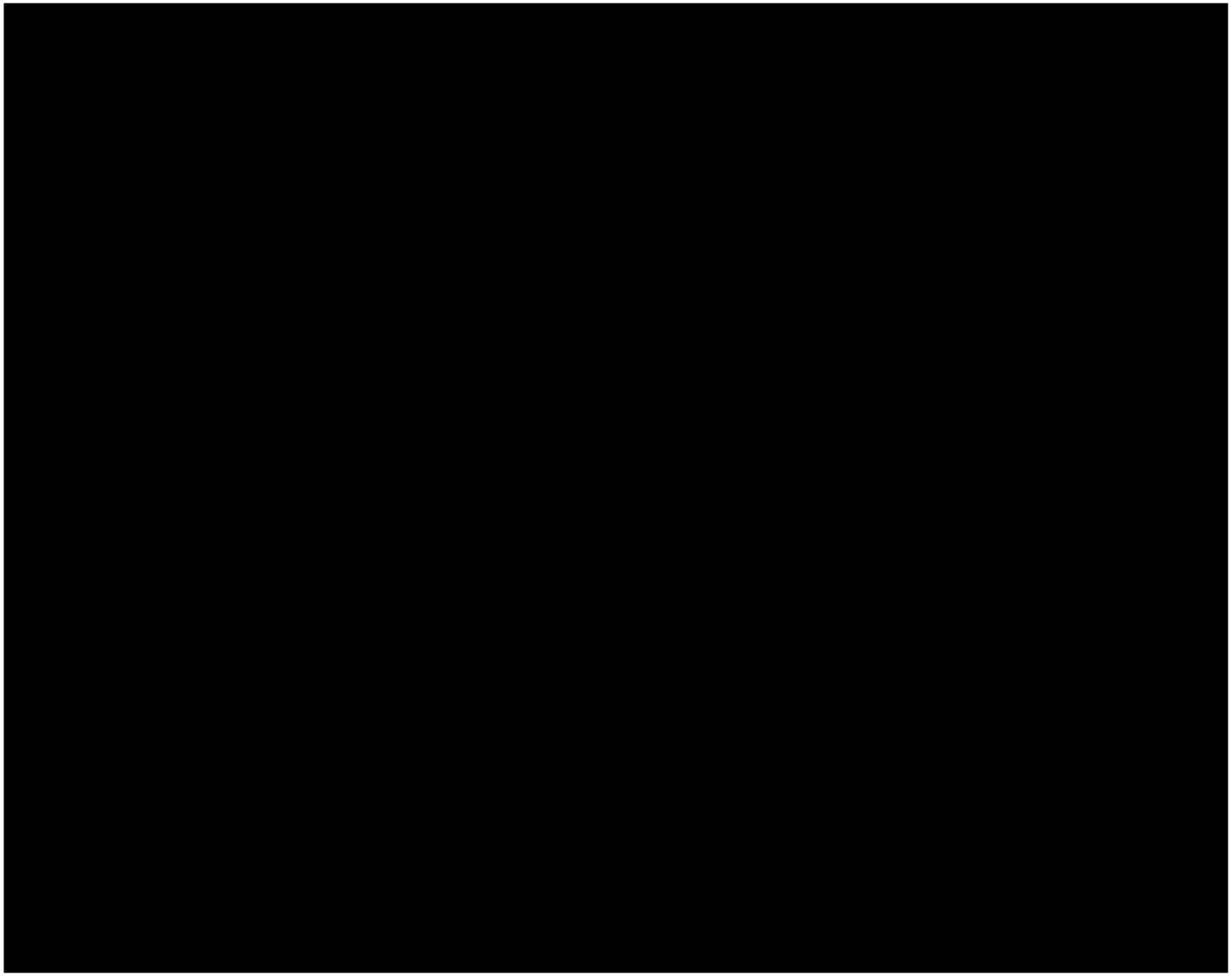
Sous-traitants	Missions	Référence de la convention	Données accessibles
Atos	Développement du traitement	Annexe du cahier des charges administratives particulières (marché	Toutes les données conservées sur
Sopra Steria			
Idakto			

[45] A ce titre, la donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour retrouver ces traces.

Idemia		public n°2020-0272, Lots 1, 2 et 4)	le serveur du SGIN
Opérateur à désigner	Mise sous pli du document contenant le code d'activation destiné à être envoyé aux usagers	-	Nom Nom d'usage Prénom(s) Adresse postale

E. En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Le traitement s'inscrit dans le cadre de l'interopérabilité du nœud eIDAS. il n'y a pas de transfert de données en dehors de l'Union européenne.



IV. Avis du délégué à la protection des données

Remarques de M. Fabrice Mattatia – Délégué à la Protection des Données - Ministère de l'Intérieur

Voir avis n° 21-000873-D du 2 juillet 2021.

V. Validation des responsables du traitement

Le responsable du traitement, Monsieur le secrétaire général du ministère de l'intérieur, atteste que la présente analyse décrit la mise en œuvre du traitement. Le responsable du traitement estime le niveau des risques résiduels pour les droits et les libertés des personnes concernées comme suffisamment faible et acceptable et s'engage à traiter les données conformément à la présente analyse, au règlement général sur la protection des données et à la loi n° 78-1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Pour l'ANTS, Madame la Directrice, atteste que la présente analyse décrit la mise en œuvre du traitement. Le responsable du traitement estime le niveau des risques résiduels pour les droits et les libertés des personnes concernées comme suffisamment faible et acceptable et s'engage à traiter les données conformément à la présente analyse, au règlement général sur la protection des données et à la loi n° 78-1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Annexe 2 – Abréviation

ANSSI	Autorité nationale de sécurité des systèmes d'information
ANTS	Agence nationale des titres sécurisés
BQA	Bureau qualification et agrément
CAN	*Card access number*
CGU	Conditions générales d'utilisation
CNIL	Commission nationale de l'information et des libertés
DNUM	Direction nationale du numérique
DR	Dispositif de recueil
eIDAS	Electronic IDentification Authentication and trust Services ou règlement (UE) n°910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur
HSM	*Hardware Security Module* ou boites noires transactionnelles
MRZ	*Machine-readable zone*
NFC	*Near Field Communication*
PACE	*Password Authenticated Connection Establishment*
PSSI	Politique de sécurité des systèmes d'information de l'Etat
RGS	Référentiel général de sécurité
SGIN	Service de garantie de l'identité numérique
SMS	Message sur *ordiphone*
SOD	*Security object*
TMA	Tierce maintenance applicative