Synthèse de l'AIPD du 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 (secrétaire général)
L'Agence nationale des titres sécurisés (ANTS)

Service gestionnaire
Programme interministériel France identité numérique

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

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.

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

I. Un besoin croissant de sécurisation des identités en ligne

Les démarches dématérialisées font aujourd'hui l'objet d'un usage massif.

II. L'État, garant de l'identité dans le monde numérique

L'État apparaît comme le garant de l'identité des citoyens dans le monde numérique. Dans son rapport de juin 2020[4], 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*. »

La CNIL, elle-même, dans sa délibération du 11 février 2021[5] 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'État 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*. »

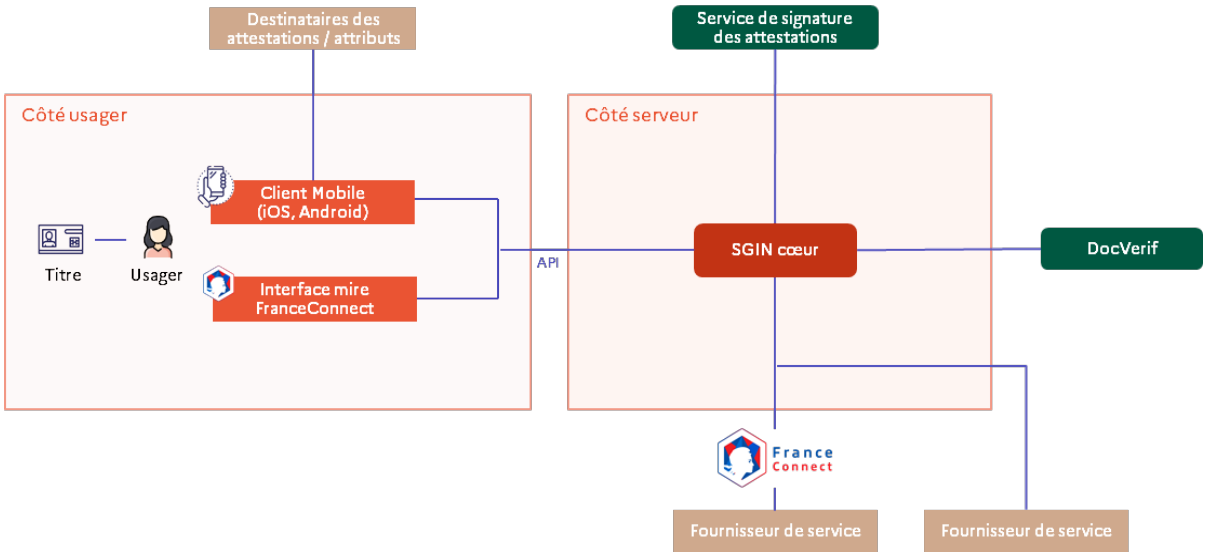
III. La mission de la direction du programme interministériel France identité numérique

Dès 2018, l'État s'est engagé dans la préparation d'un dispositif.

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

[4] Conseil national du numérique, *Identités numériques. Clés de voûte de la citoyenneté numérique*, juin 2020.
[5] 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.

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



V. 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
- La simplicité d'utilisation
- La minimisation de la collecte des données à caractère personnel
- La transparence
- La sécurité

VI. Les usages du moyen d'identification électronique

Le moyen d'identification électronique proposé par l'État 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'État (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.

II. 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 :

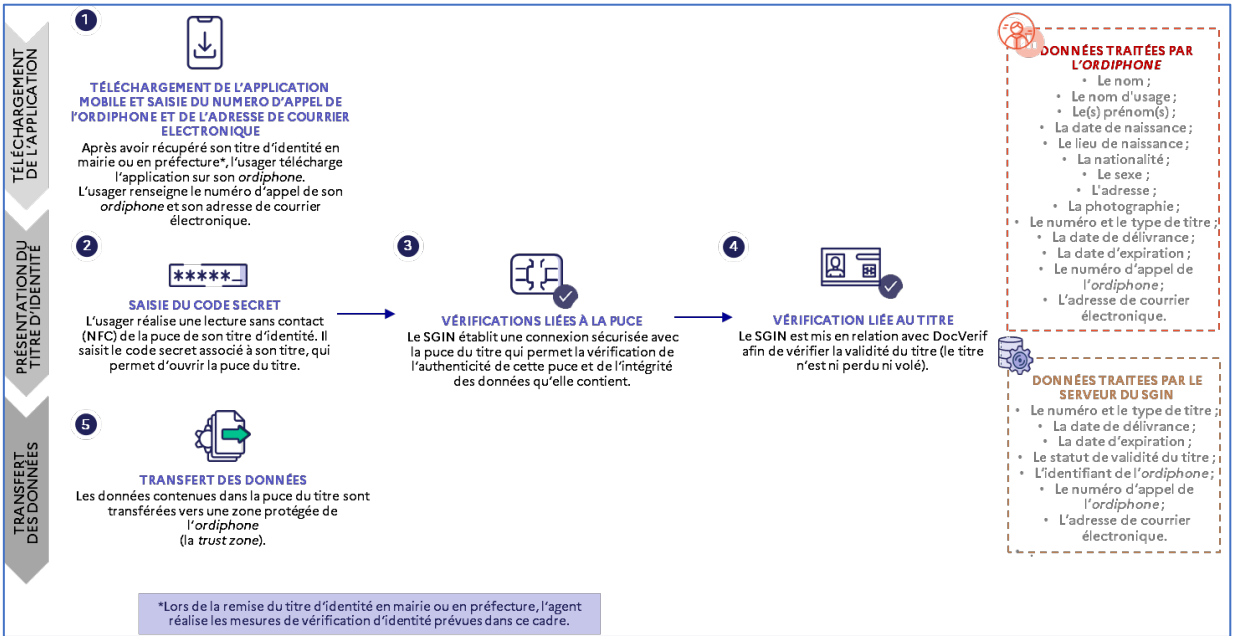
- sa délivrance ;
- son utilisation ;
- sa gestion.

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[6]
Remise du titre en mairie ou en préfecture par un agent, après réalisation des mesures de vérification d'identité prévues dans ce cadre[7].	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
Téléchargement de l'application par l'usager sur son *ordiphone*.	
Lecture NFC du composant électronique du titre d'identité. Saisie de son code secret[11] 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[12] et de l'intégrité des données contenues dans ce composant électronique[13].	
Vérification de la validité du titre d'identité[14].	

[6] A l'exception de l'identifiant de l'o*rdiphone,* 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.

[7] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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).

Description du processus	Données traitées[6]
Transfert des données contenues dans le composant électronique du titre d'identité vers une zone protégée de l'*ordiphone* (la « trust zone »).	L'identifiant de l'*ordiphone*[8] Le numéro d'appel de l'*ordiphone*[9] L'adresse de courrier électronique[10] Le statut de validité du titre (valide/invalide/inconnu)

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'État. 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

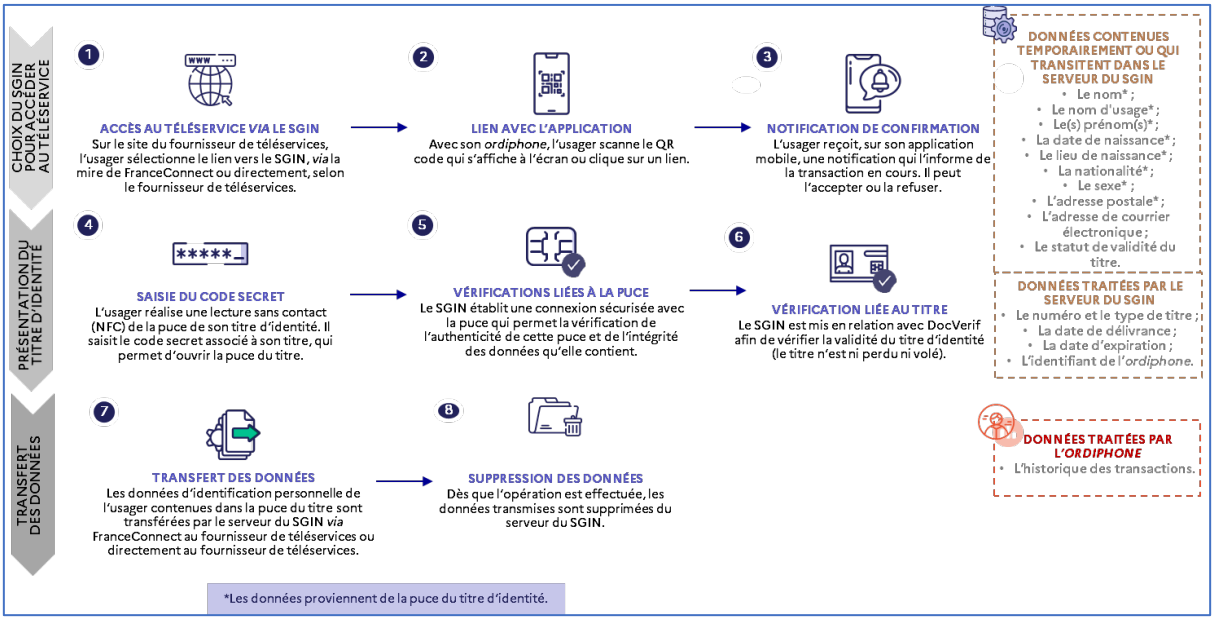
a. Les authentifications permettant l'accès à des téléservices exigeant un niveau de garantie élevé

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

[8] Cette donnée est générée par le traitement.
[9] Cette donnée est renseignée par l'usager lors de la création du moyen d'identification électronique.
[10] Cette donnée est renseignée par l'usager lors de la création du moyen d'identification électronique.



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[15] L'identifiant de l'*ordiphone*
Scan par l'usager *via* son *ordiphone* d'un QR code ou clic sur un lien pour ouvrir l'application mobile[16]. 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.	

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

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

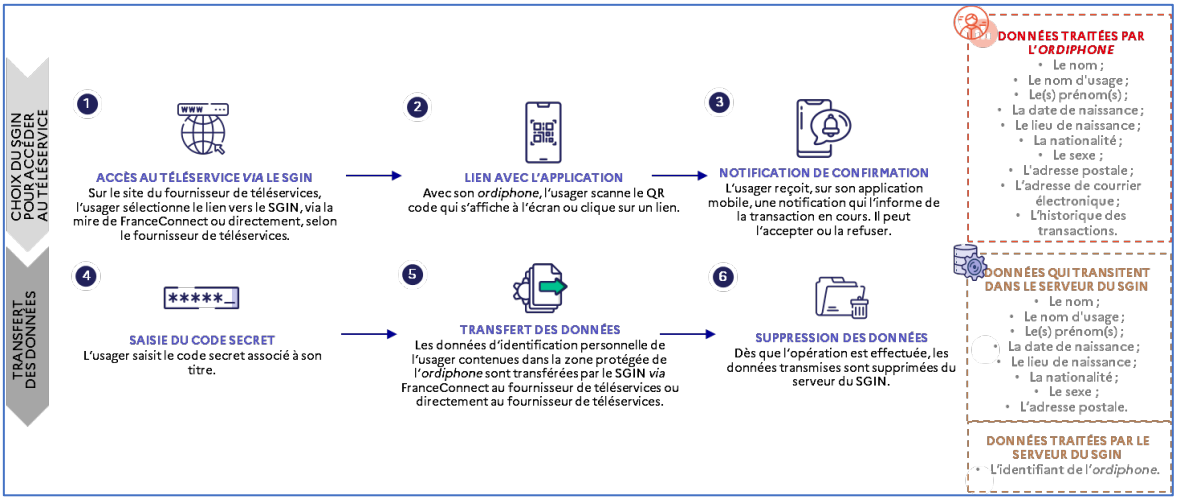
Description du processus	Données traitées
Vérification de l'authenticité du composant électronique du titre d'identité et de l'intégrité des données contenues dans ce composant électronique.	Le numéro de titre Sa date de délivrance Sa date d'expiration Le statut de validité du titre (valide/invalide/inconnu)
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.

Schéma général

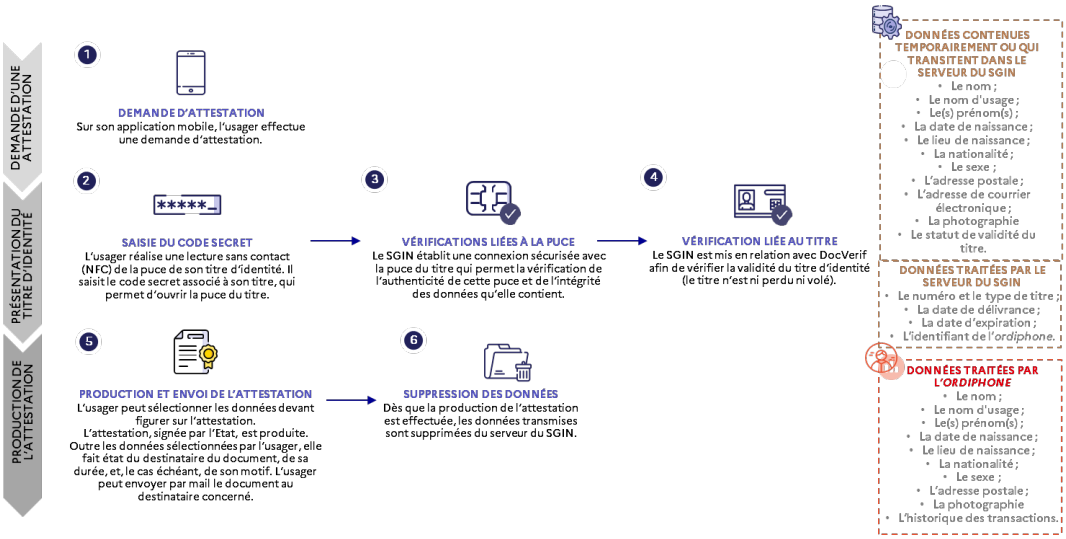


2. Les authentifications permettant l'obtention d'attestations électroniques d'attributs d'identité ou d'un attribut d'identité

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
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	

Description du processus	Données traitées
Obtention de l'attestation électronique d'attributs d'identité, signé par l'État[17], 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.	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)
Envoi par voie électronique du document par l'usager au destinataire concerné	

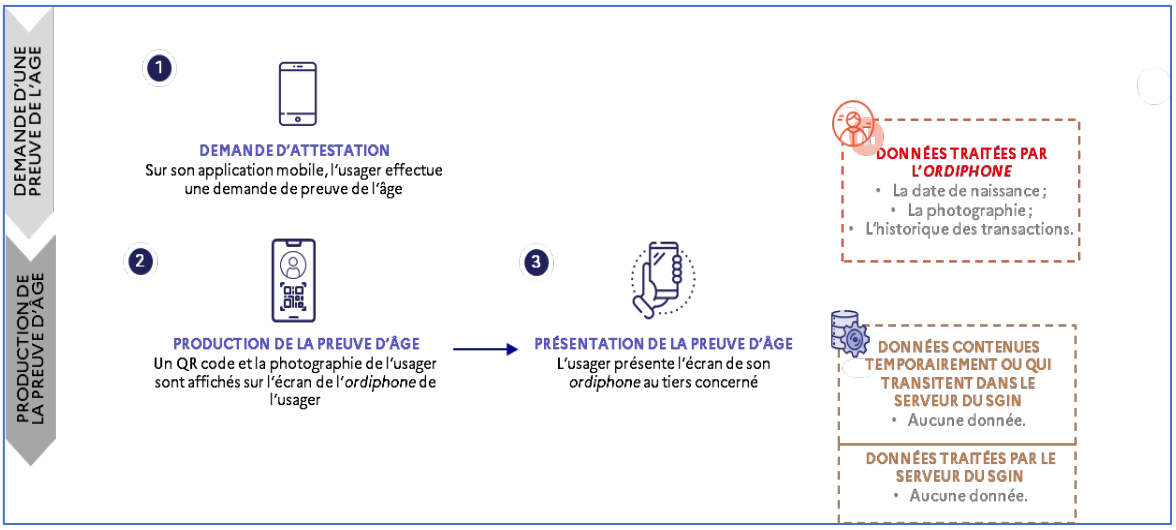
3. La preuve de l'âge ou de la majorité

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.

Schéma général

[17] La signature par l'État de l'attestation électronique est systématique. Le document électronique est signé par l'État 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.



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[18] et de la photographie[19] 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*[20]. Aucune donnée n'est conservée, ni par le destinataire, ni dans l'application de l'usager.

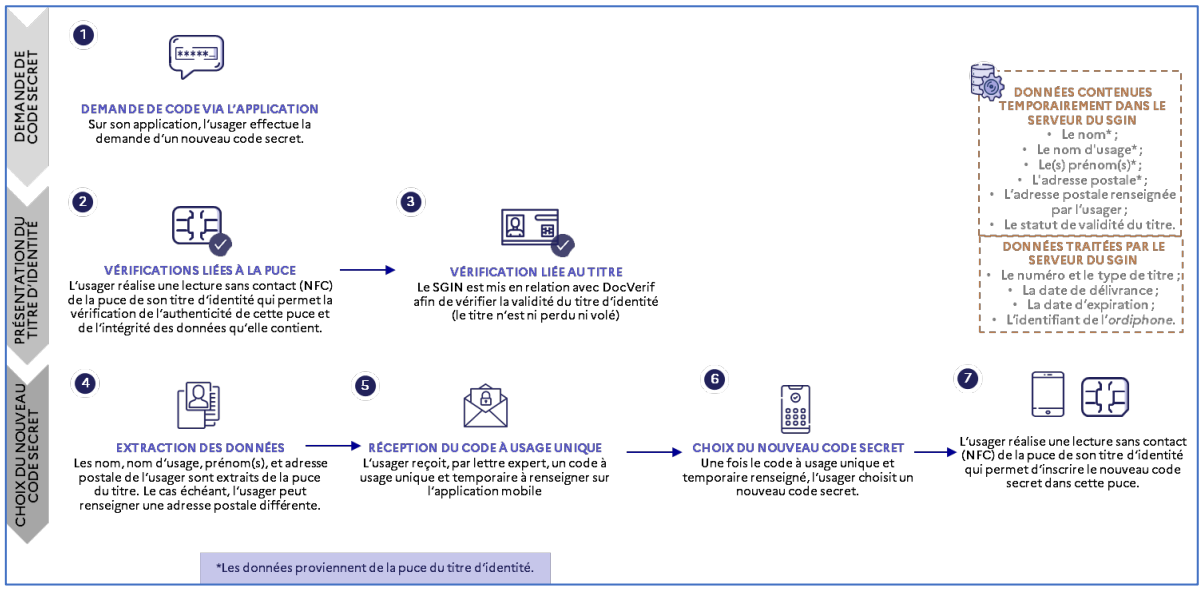
C. Le processus de gestion du moyen d'identification électronique

1. Perte ou blocage du code secret

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

[18] Le QR code s'appuie sur le standard 2D-DOC qui inclut une signature électronique.
[19] 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.
[20] 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
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[21] d'un code à usage unique et temporaire à renseigner sur l'application mobile.	
Lecture du titre et choix d'un nouveau code secret[22].	

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

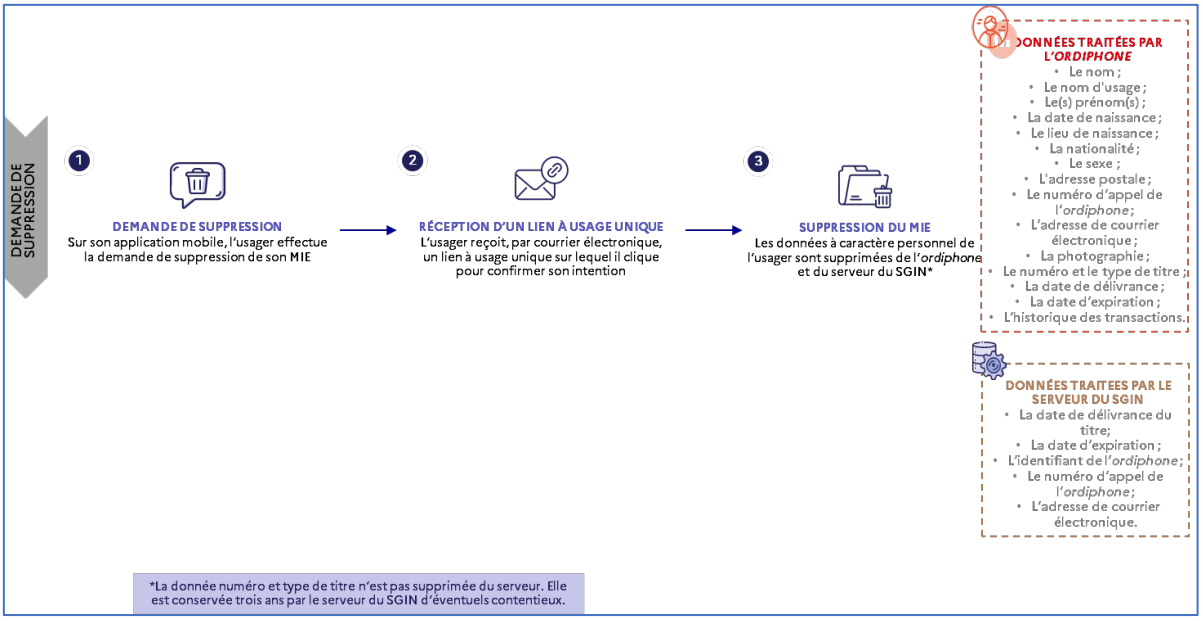
[22] Le choix du code secret doit obéir aux principes suivants :
- les motifs de deux ou trois chiffres (exemple : 119117, 123123) ou les suites de quatre chiffres (exemple : 0123, 1234, 4567) sont interdits ;
- le code secret doit contenir au moins trois chiffres différents ;

Description du processus	Données traitées
	L'identifiant de l'*ordiphone* 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)
Réception par l'usager d'un lien à usage unique, par courrier électronique, sur lequel il doit cliquer pour confirmer son intention.	

- le code secret doit être différent de la date de naissance de l'usager (au format JJMMAA).

Description du processus	Données traitées
Suppression des données à caractère personnel de l'*ordiphone* et du serveur[23].	La date de naissance Le lieu de naissance La nationalité Le sexe L'adresse postale 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'*ordiphone* L'adresse de courrier électronique

3. La révocation du moyen d'identification électronique

En cas de perte ou de vol de son *ordiphone*[24], l'usager peut révoquer son moyen d'identification électronique.

Schéma général

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

[24] 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.

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. 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
2. Le système d'information d'un opérateur postal
3. FranceConnect
4. Les fournisseurs de services qui ne sont pas interfacés avec FranceConnect
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.
- le service d'horodatage qualifié eIDAS,
- le service de relai de messagerie électronique

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.

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.

III. 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[25] ainsi que des moyens utilisés pour réaliser cette identification électronique[26] 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'État 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'État. Ce décret est en cours de rédaction ;
- Le règlement sur la carte nationale d'identité[27] impose aux États-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 ;

[25] 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* ».
[26] 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* ».
[27] 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.

- 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)[28] 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 ;
- 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.

[28] 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).

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[29] si ces derniers suppriment leur moyen d'identification électronique *via* l'application mobile ou désinstallent 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'État. 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.

En proposant un moyen d'identification électronique sécurisé, gratuit et inclusif, adossé à la carte nationale d'identité comprenant un composant électronique, l'État 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.

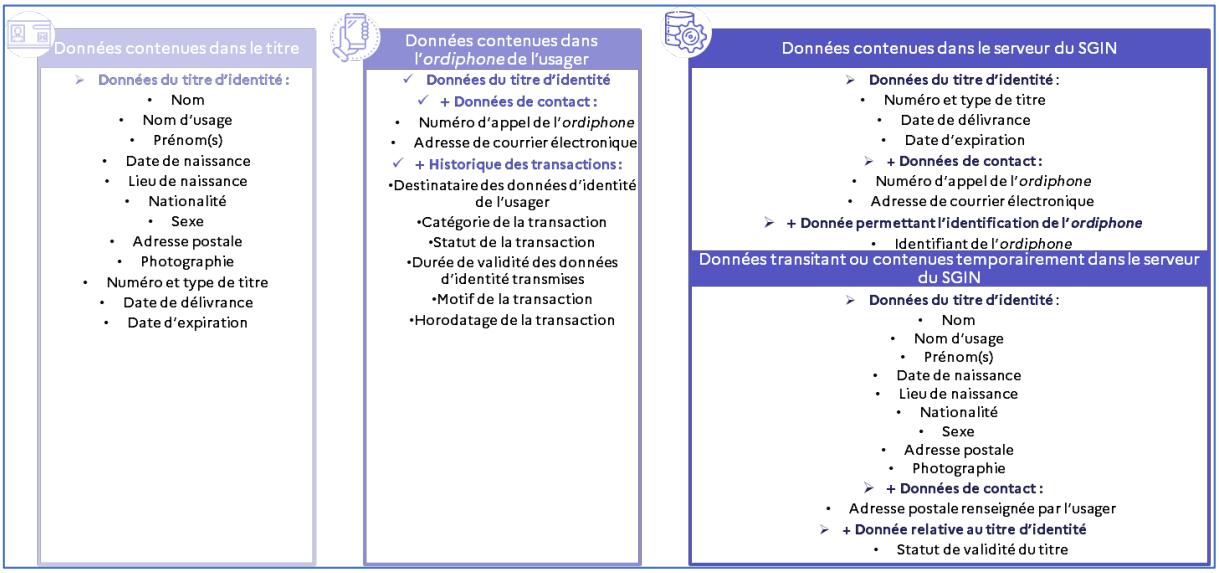
L'État a également pour mission de lutter contre l'usurpation d'identité. Le moyen d'identification électronique régalien, qui vise les niveaux de garantie

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

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		

Catégorie de données	Données	Rôle	Origine	Durée de conservation
	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	Renseignement par les usagers	Cinq ans maximum (durée de validité de l'identité numérique selon le RGS)
	Adresse de courrier électronique	Données transmises au serveur du SGIN pour les échanges avec les usagers et la sécurisation des processus		
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	Conservation des cinq dernières transactions dans la limite de cinq ans (durée de validité de l'identité numérique selon le RGS)
	Catégorie de la transaction			
	Statut de la transaction			
	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

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

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

Catégorie de données	Données	Rôle	Origine	Durée de conservation
		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
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[30].

Les données à caractère personnel sont supprimées de l'*ordiphone* et du serveur du SGIN[31] 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[32] lorsque les usagers :

- Désinstallent l'application mobile :
- 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 ;

[30] 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.
[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.
[32] La donnée numéro et type de titre n'est pas supprimée du serveur. Elle est conservée trois ans pour le traitement d'éventuels contentieux.

- La politique de sécurité et de confidentialité du traitement.

À 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 ;
- 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[33].

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

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

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.

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

IV. Avis du délégué à la protection des données

L'AIPD du SGIN a fait l'objet d'un avis rendu par le délégué à la protection des données du ministère de l'Intérieur le 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.

VI. Annexe – 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