L14 – Processus d'authentification et d'identification fID et architecture fonctionnelle du système d'identification cible

Projet de services de conseil pour le développement de la stratégie, la conception organisationnelle et l'architecture technique, l'acquisition de services informatiques et l'appui à la gestion de projet pour la mise en œuvre du système fID

Janvier 2024 Version 1.3

Contacts

Contacts principaux – Equipe technique WURI Bénin			
Nom	M. Jean AHOLOU		
Rôle	Coordonnateur	Mobile	+229 95 84 93 80
E-mail	aholjaen@yahoo.fr	Site Web	
Nom	M. Thierry ADOKO		
Rôle	Spécialiste Suivi-Evaluation	Mobile	+229 97 38 67 58
E-mail	thibagbag@gmail.com	Site Web	
Nom	M. Franck AHOUANSOU		
Rôle	Expert en architecture/infrastructure	Mobile	+229 97 17 47 20
E-mail	franckolande@gmail.com	Site Web	
Nom	M. Edgar AYENA		
Rôle	Expert architecture développement logiciel	Mobile	+229 95 80 53 26
E-mail	ayenadedg@gmail.com	Site Web	
Nom	M. Marius Bellor GANHOUNOUTO		
Rôle	Ingénieur Réseaux Informatique et Télécoms	Mobile	+229 97 33 47 02
E-mail	bellorganhounouto@gmail.com	Site Web	

Contacts principaux – EY & EDS			
Nom	M. Mounir GHAZALI		
Rôle	Associé	Mobile	+216 23 44 91 24

E-mail	Mounir.Ghazali@tn.ey.com	Site Web	www.ey.com
Nom	M. Eric DA SILVA		
Rôle	Associé	Mobile	+229 97 27 57 57
E-mail	e.dasilva@eds-telecom.net	Site Web	www.eds-telecom.net
Nom	M. Wissem GHAZAOUI		
Rôle	Associé	Mobile	+216 29 67 78 64
E-mail	Wissem.Ghazaoui@tn.ey.com	Site Web	www.ey.com
Nom	M. Mohamed Lamine Touré	Mobile	
Rôle	Senior Manager	Mobile	+224 610 00 16 10
E-mail	Mohamed.Lamine.Toure@gn.ey.com	Site Web	www.ey.com

Contrôle des documents

Nom du projet :	Projet de services de conseil pour le développement de la stratégie, la conception organisationnelle et l'architecture technique, l'acquisition de services informatiques et l'appui à la gestion de projet pour la mise en œuvre du système fID
Représentant client :	Jean AHOLOU (Coordonnateur du projet WURI Bénin)
Numéro de contrat :	0227 MEF/PR/ANIP/WURI-BENIN/SPM/DNCMP/SP
Date de début du projet :	Février 2022
Date initiale de fin du projet :	Mai 2023
Rapport EY N° :	L14

Tableau 1 : Résumé du projet

	Nom	Fonction
WURI	JEAN AHOLOU	COORDONNATEUR DU PROJET WURI BENIN
	M. FRANCK AHOUANSOU	EXPERT EN ARCHITECTURE / INFRASTRUCTURE
	THIERRY ADOKO	SPECIALISTE EN SUIVI-EVALUATION
	EDGAR AYENAA	EXPERT ARCHITECTURE DEVELOPPEMENT LOGICIEL
	M. MARIUS BELLOR GANHOUNOUTO	INGENIEUR RESEAUX INFORMATIQUE ET TELECOMS
ANIP	MARIEL ATTONDE	DSI -ANIP
	M. RÉGIS S. JEAN-ROMUALD SOUMAHO	WURI- ANIP
	M. AURELE QUENUM	WURI- ANIP
	M. JOSIAS RANTI AGOSSOU	ADMINISTRATEUR SYSTEME
ASIN ASIN	M. ISAIE DJROLO	ASIN – MANAGER DES OPERATIONS PKI
ASIN	M. ADJINAKOU ARISTIDE	ASIN

	M. THIERRY AHOUASSOU	ASIN – SPECIALISTE PROJET ET STRATEGIE
	M. CHARLES MUGUISHA	ASIN - ARCHITECTE SI
MASM	M. VINCENT DE PAUL MEGNIGBETO	MASM- DIRECTEUR DES SYSTEMES D'INFORMATION
	M. AGBAFFA-PADONOU FEMI NOAH	MINISTERE DES AFFAIRES SOCIALES ET DE LA MICROFINANCE
MND	M. SONGBIAN ZIME	MINISTERE DU NUMERIQUE ET DE LA DIGITALISATION
	M. HONTINFINDE REGIS DONALD	MINISTERE DU NUMERIQUE ET DE LA DIGITALISATION
EY & EDS	M.MOUNIR GHAZALI	ASSOCIE EY
	M.ERIC DA SILVA	ASSOCIE EDS T&C
	M.WISSEM GHAZAOUI	ASSOCIE EY
	M.MOHAMED LAMINE TOURE	SENIOR MANAGER EY

Tableau 2 : Membres clés de l''équipe de projet

Contrôle de versions

Version #	Date	Organisation	Remarques
1.0	17/10/2023	EY-EDS T&C	Livrable L14 : Processus d'authentification et d'identification fID
1.1	21/11/2023	EY-EDS T&C	Livrable L14 : Processus d'authentification et d'identification fID
1.2	29/12/2023	EY-EDS T&C	Mise à jour du livrable suite aux commentaires de la BM
1.3	17/01/2024	EY-EDS T&C	Mise à jour du livrable suite au commentaire de la BM

Tableau 3 : Contrôle de versions

Glossaire des termes

Terme	Description
ANIP	Agence Nationale d'Identification des Personnes
API	Application Programming Interface
BPMN	Business Process Model and Notation
e-KYC	Electronic Know Your Customer
fID	Fondamental identification
HSM	Hardware Security Module
HSM	Hardware Security Module
IDV	ID Virtuel
MFA	Authentification multifacteurs
NPI	Numéro d'Identification Personnelle
OTP	One Time Password
PKI	Public Key Infrastructure
POS	Plan d'Occupation des Sols
RNPP	Registre National des Personnes Physiques
WURI	West Africa Unique Identification for Regional Integration and Inclusion

Table des Matières

Table des figures

Liste des tableaux

Contexte, objectif du livrable

Les processus d'enregistrement et d'authentification sont au cœur des enjeux de mise en place d'un système d'identification fiable et inclusif. En effet l'atteinte d'une couverture totale de la population garantissant une meilleure qualité des services publics aux citoyens/résidents béninois, est fortement tributaire de la fiabilité et de l'efficacité des processus de l'enregistrement et de l'authentification.

Ce document vient consolider les livrables qui le précèdent, notamment celui portant sur la conception de l'architecture cible du système en sa globalité « L9 - Conception de l'architecture cible du système fID ». Il a pour objectif d'apporter les détails nécessaires à une compréhension plus fine des processus d'enregistrement et d'authentification.

Structure du livrable

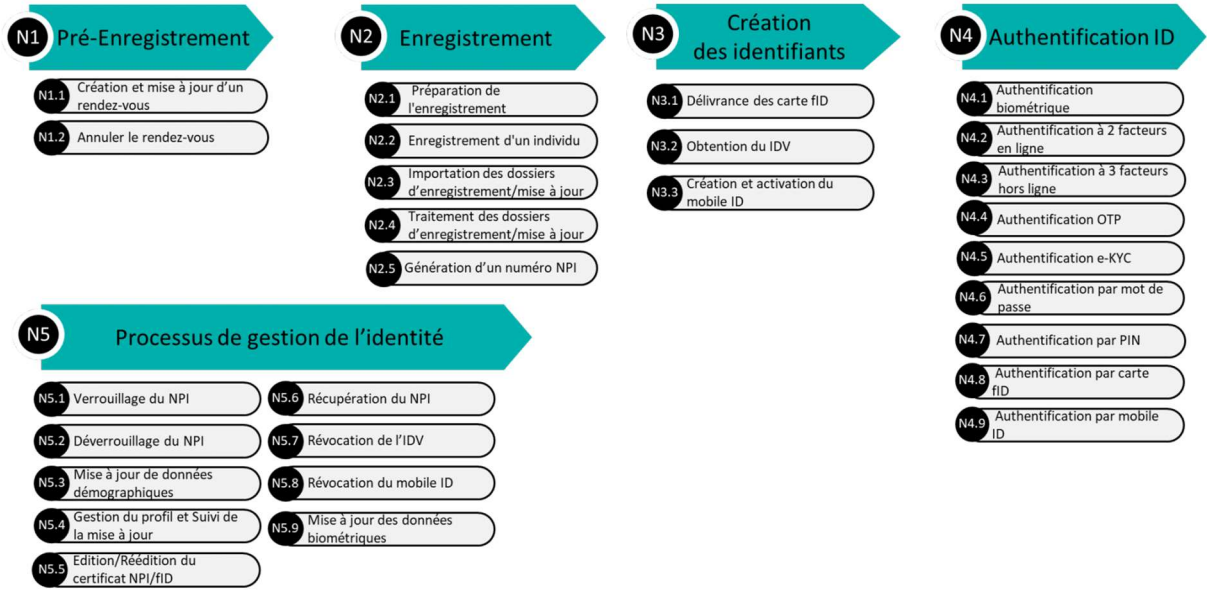
Ce livrable est réparti en 9 chapitres :

- Le premier chapitre se penche sur les fondamentaux du BPMN 2.0, expliquant sa pertinence, ses caractéristiques et comment il s'intègre dans le contexte du Système d'identification. Ce chapitre rappelle également les différents acteurs impliqués et définit les différents termes utilisés tout au long de ce document.
- Le 2ème chapitre aborde l'un des éléments clés du système d'identification cible : les processus d'enregistrement. Pour garantir une efficacité optimale et une compréhension claire, ces processus sont scindés en plusieurs étapes distinctes, notamment le pré-enregistrement et l'enregistrement suivis de l'importation des dossiers. Dans ce chapitre, ces processus ont été présentés et modélisés en détail pour offrir une vue holistique de leur fonctionnement et de leur importance.
- Le 3ème chapitre se focalise sur les mécanismes essentiels qui permettent aux utilisateurs d'accéder aux services : la création de compte et la procédure de connexion. Quatre sous-processus distincts ont été présentés et modélisés en se concentrant sur les spécificités liées respectivement aux comptes Mobile et au portail fID.
- Le 4ème chapitre présente les processus d'obtention des différentes identités notamment l'identité virtuelle, l'identité électronique et la carte fID.
- Les chapitres 5 et 6 examinent en détail les méthodes d'authentification, qu'elles soient en ligne ou hors ligne.
- Le chapitre 7 détaille les étapes que les citoyens/résidents doivent suivre pour accéder à des services liés à leur identité, tels que la révocation de l'IDV, la révocation du mobile ID, la réédition/édition du certificat fID, la mise à jour des données d'identification biométriques et démographiques, etc.

- Le 8ème chapitre se centre sur l'architecture fonctionnelle du Système d'identification basée sur le plan d'occupation des sols SI, une représentation haut niveau qui se détache des complexités techniques pour se concentrer sur les fonctionnalités essentielles.
- Le 9ème et dernier chapitre propose des suggestions visant à optimiser encore d'avantage l'expérience utilisateur.

Périmètre du livrable

Le périmètre de ce livrable englobe la modélisation des processus essentiels relatifs au préenregistrement, à l'enregistrement, à l'authentification, ainsi qu'à la gestion de l'identité, tous formalisés conformément au standard BPMN 2.0, comme illustré dans la figure ci-dessous



Les principaux enseignements

1. Afin de faciliter le processus d'enregistrement aux citoyens et résidents béninois et afin de mieux fluidifier ce process, un process de pré-enregistrement pourra être instauré.

Un des plus grands avantages de ce process est que toutes les données soumises seront transmises directement au centre d'enregistrement choisi avant même le rendez-vous. Ainsi, lors de la visite de l'individu, le personnel pourra accéder instantanément à ces informations, rendant le processus d'enregistrement beaucoup plus rapide et efficace.

En somme, cette évolution représente une étape significative vers la modernisation des services administratifs, garantissant une expérience utilisateur améliorée et une gestion plus simplifiée des enregistrements.

2. L'authentification du citoyen/résident est un mécanisme essentiel pour assurer la sécurité des données et l'accès au système d'identification. Cependant, il est crucial de distinguer deux types d'authentification qui comportent des contraintes différentes :

- Authentification en ligne : cette modalité exige que le citoyen/résident soit connecté à Internet (authentification par OTP, par PIN, par mot de passe et à 2 facteurs)
- Authentification hors ligne :
    - Citoyen hors ligne se réfère à un déplacement physique du citoyen/résident chez le fournisseur de service pour confirmer son identité, dans ce cas, les modalités d'authentification suivantes sont possibles : authentification par carte fID authentification biométrique, authentification e-kYC et authentification par mobile ID.
    - Fournisseur de service hors ligne implique que, outre le fait que le citoyen soit physiquement présent lors de la procédure, le fournisseur de service n'a pas accès à une connexion Internet. Malgré l'absence de connectivité en ligne, le fournisseur de service doit néanmoins être en mesure d'authentifier le citoyen.

Ce sont donc ces deux modalités qui sont développées dans ce document.

A noter que les agents de l'identification et le fournisseur de service sont nécessairement connecté en ligne pour pouvoir vérifier et valider les identités des citoyens/résidents.

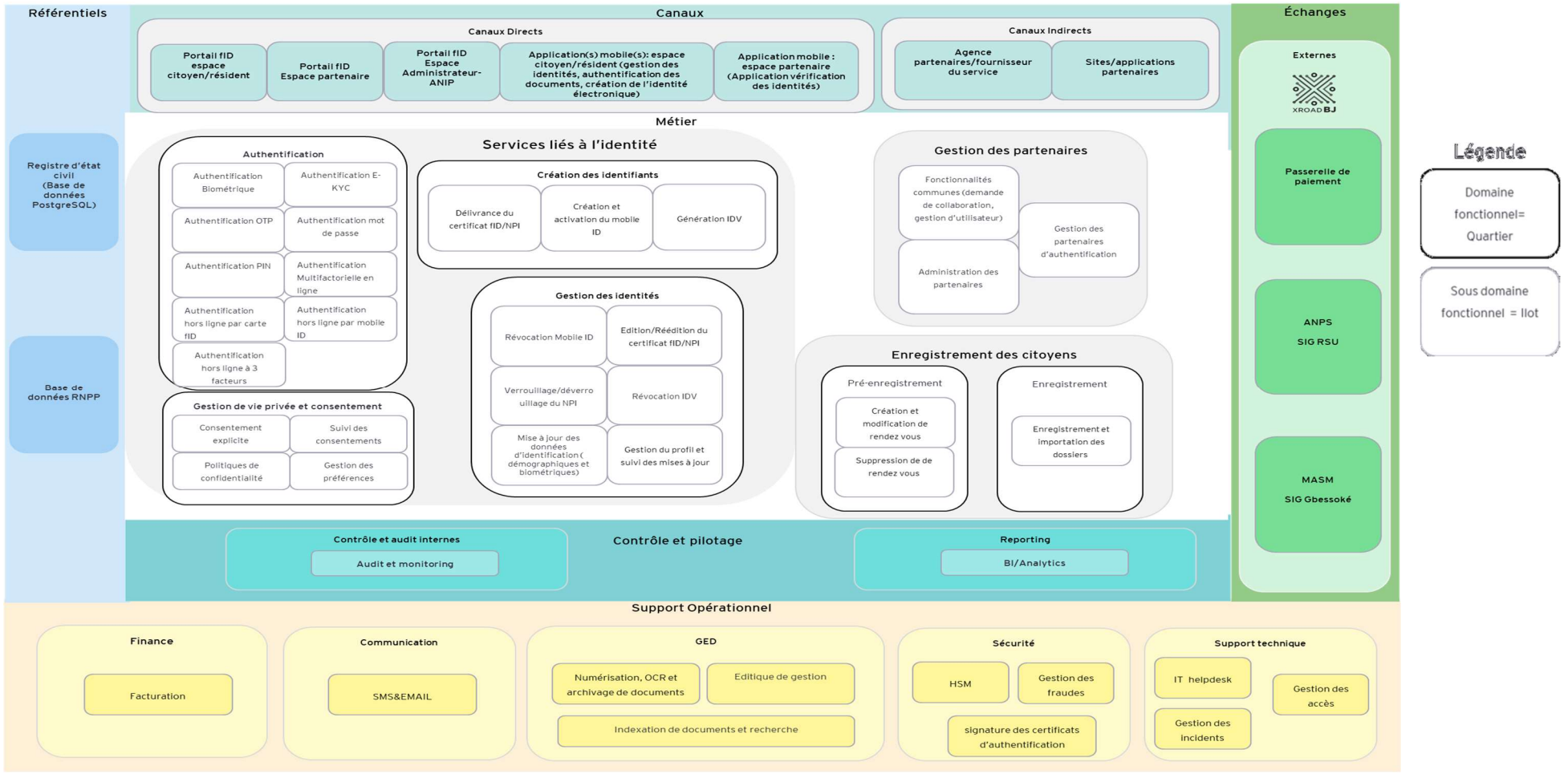
3. Quelques recommandations ont été proposées afin d'améliorer l'expérience utilisateur, de lui faciliter son quotidien et de lui simplifier les démarches administratives et ceci en proposant d'associer à l'identifiant citoyen un portefeuille numérique complet, véritable coffre-fort numérique.

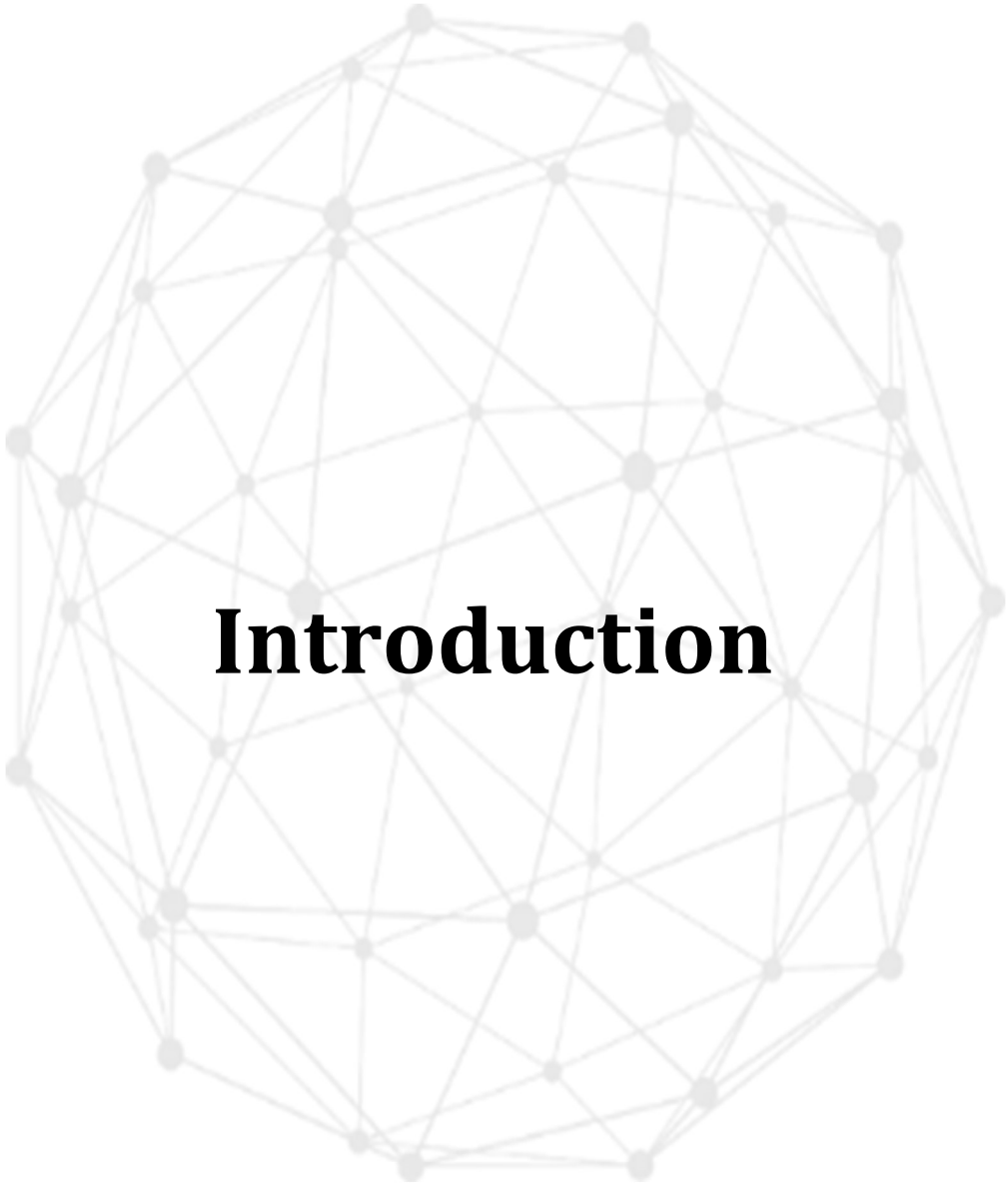
L'architecture fonctionnelle cible du système d'identification

Ayant modélisé en détail les processus métiers liés à l'identification et l'authentification lors de la rédaction de ce document, nous nous focaliserons par la suite sur la vue fonctionnelle qui se concentrera sur les fonctionnalités requises pour soutenir les processus métiers précédemment identifiés.

L'objectif est de comprendre comment le Système d'identification doit être conçu pour répondre aux besoins métiers, sans aborder les spécificités techniques ou applicatives, à savoir que l'architecture technique devra être proposée par le prestataire pour répondre aux besoins fonctionnels et métiers justement exprimés dans ce livrable

L'architecture fonctionnelle proposée ci-dessous se compose de six zones distinctes, et pour chacune de ces zones, nous avons défini un domaine fonctionnel spécifique, connu sous le nom de Quartier fonctionnel. Chacun de ces domaines fonctionnels est subdivisé en sous-domaines fonctionnels, comme précisé dans le document intitulé "L9 - Conception de l'architecture cible du système fID".


Référentiels
Registre d'état civil (Base de données PostgreSQL)
Base de données RNPP
Canaux
Canaux Directs
Portail fID espace citoyen/résident
Portail fID Espace partenaire
Portail fID Espace Administrateur-ANIP
Application(s) mobile(s): espace citoyen/résident (gestion des identités, authentification des documents, création de l'identité électronique)
Application mobile : espace partenaire (Application vérification des identités)
Canaux Indirects
Agence partenaires/fournisseur du service
Sites/applications partenaires
Métier
Authentification
Authentification Biométrique
Authentification E-KYC
Authentification OTP
Authentification mot de passe
Authentification PIN
Authentification Multifactorielle en ligne
Authentification hors ligne par carte fID
Authentification hors ligne par mobile ID
Authentification hors ligne à 3 facteurs
Services liés à l'identité
Création des identifiants
Délivrance du certificat fID/NPI
Création et activation du mobile ID
Génération IDV
Gestion des identités
Révocation Mobile ID
Edition/Réédition du certificat fID/NPI
Verrouillage/déverrouillage du NPI
Révocation IDV
Mise à jour des données d'identification (démographiques et biométriques)
Gestion du profil et suivi des mises à jour
Gestion de vie privée et consentement
Consentement explicite
Suivi des consentements
Politiques de confidentialité
Gestion des préférences
Gestion des partenaires
Fonctionnalités communes (demande de collaboration, gestion d'utilisateur)
Administration des partenaires
Gestion des partenaires d'authentification
Enregistrement des citoyens
Pré-enregistrement
Création et modification de rendez vous
Suppression de de rendez vous
Enregistrement
Enregistrement et importation des dossiers
Contrôle et audit internes
Audit et monitoring
Contrôle et pilotage
Reporting
BI/Analytics
Échanges
Externes
XROAD BJ
Passerelle de paiement
ANPS
SIG RSU
MASM
SIG Gbessoké
Légende
Domaine fonctionnel= Quartier
Sous domaine fonctionnel = Ilot
Support Opérationnel
Finance
Facturation
Communication
SMS&EMAIL
GED
Numérisation, OCR et archivage de documents
Editique de gestion
Indexation de documents et recherche
Sécurité
HSM
Gestion des fraudes
signature des certificats d'authentification
Support technique
IT helpdesk
Gestion des incidents
Gestion des accès



1 Introduction

1. Introduction

Les processus d'enregistrement et d'authentification sont au cœur des enjeux de mise en place d'un système d'identification fiable et inclusif. En effet l'atteinte d'une couverture totale de la population garantissant une meilleure qualité des services publics aux citoyens béninois, est fortement tributaire de la fiabilité et de l'efficacité des processus de l'enregistrement et de l'authentification.

Ce document vient consolider les livrables qui le précèdent, notamment celui portant sur la conception de l'architecture cible du système en sa globalité « L9 - Conception de l'architecture cible du système fID ». Il a pour objectif d'apporter les détails nécessaires à une compréhension plus fine des processus d'enregistrement et d'authentification.

Le processus global représente l'ensemble des étapes conceptuelles qu'un citoyen/résident doit suivre pour accéder à un service. Ces étapes impliquent l'intervention du système d'identification géré par l'ANIP ainsi que les fournisseurs de services qui peuvent être des institutions publiques, privés ou encore des plateformes de services en ligne.

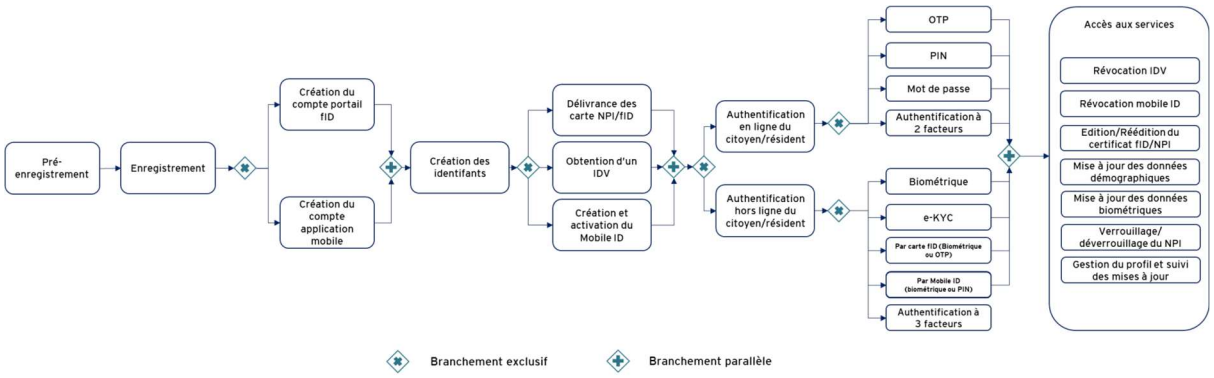


Figure 1 : Processus global des activités

Ci-dessus le processus global synthétisant toutes les activités allant du pré-enregistrement jusqu'à l'accès aux services.

Le processus d'authentification commence lorsque le citoyen/résident souhaite être enregistré l'amenant ainsi à prendre rendez-vous pour un pré-enregistrement.

Lors de ce rendez-vous, le citoyen/résident se rend au centre d'enregistrement choisi au préalable et procède à son enregistrement. Suite à cela, il reçoit un numéro NPI qui lui permet de s'identifier sur le portail fID et l'application mobile pour accéder à un service spécifique.

Selon le mode d'authentification choisi, en ligne ou hors ligne, le citoyen/résident fournit les informations nécessaires au fournisseur de service. Le fournisseur, à son tour, sollicite le système d'identification pour confirmer l'identité du citoyen, en utilisant divers outils tels que le moteur de déduplication ou le SDK.

L'authentification dépend de la nature du service. Pour un service critique, une authentification multifactorielle peut être nécessaire, tandis qu'un service de moindre importance pourrait ne nécessiter qu'un seul facteur d'authentification et ceci afin de garantir un accès sécurisé et fiable aux services.

Une fois authentifié sur le portail fID ou sur l'application mobile, le citoyen/résident peut réaliser les actions suivantes :

- Obtenir un IDV
- Révoquer un IDV
- Révoquer le mobile ID
- Editer/Rééditer son certificat fID/NPI
- Mettre à jour ses données d'identification démographiques
- Mettre à jour ses données biométriques
- Verrouiller/déverrouiller son NPI
- Gérer son profil et suivre les mises à jour

Les prochaines sections de ce document détailleront davantage le processus global, en abordant les mécanismes d'enregistrement, d'authentification en ligne et hors ligne, et en discutant des méthodes telles que l'OTP, le PIN, le mot de passe et l'authentification multifactorielle. Elles exploreront également les services disponibles pour le citoyen après authentification.

Ce processus garantit que seules les personnes authentifiées et éligibles ont accès au service concerné, assurant ainsi une meilleure sécurité et plus de fiabilité de la prestation de services.

Les sections du présent document approfondiront les étapes mentionnées ci-dessus. Elles décriront en détail les processus d'enregistrement, d'authentification, qu'ils soient en ligne ou hors ligne, et traiteront des modalités d'authentification telles que l'OTP, le PIN, le mot de passe, etc. ainsi que les services offerts au citoyen une fois authentifié.

Les facteurs d'authentification peuvent être classés en trois catégories distinctes :

- Les éléments que le citoyen ou le résident possède, tels que le Numéro d'Identification Personnelle (NPI), la carte fID/NPI, le mobile ID et l'IDV.
- Les informations que le citoyen ou le résident connaît, comme le code PIN, le mot de passe et l'OTP.
- Les caractéristiques physiologiques ou biométriques qui définissent le citoyen ou le résident, telles que le visage et l'empreinte digitale.

Pour ce faire, nous nous baserons sur un standard international pour la modélisation graphique des processus d'affaires (BPMN 2.0).

1.1 Présentation du standard de modélisation graphique BPMN 2.0

BPMN 2.0 est un standard international pour la modélisation graphique des processus d'affaires dans le cadre des initiatives BPM (Business Process Management). Il fournit des symboles et des notations pour représenter les activités, les événements, les passerelles, etc permettant ainsi une représentation visuelle des processus métier.

Il offre une représentation standardisée des processus, rendant ces derniers compréhensibles à l'ensemble des parties prenantes (techniciens, managers, analystes, etc.) et facilite la communication entre les équipes techniques et métier lors de la mise en place de nouvelles solutions ou de l'amélioration des processus existants.

Ci-dessous la liste détaillée des symboles utilisés tout au long de ce document

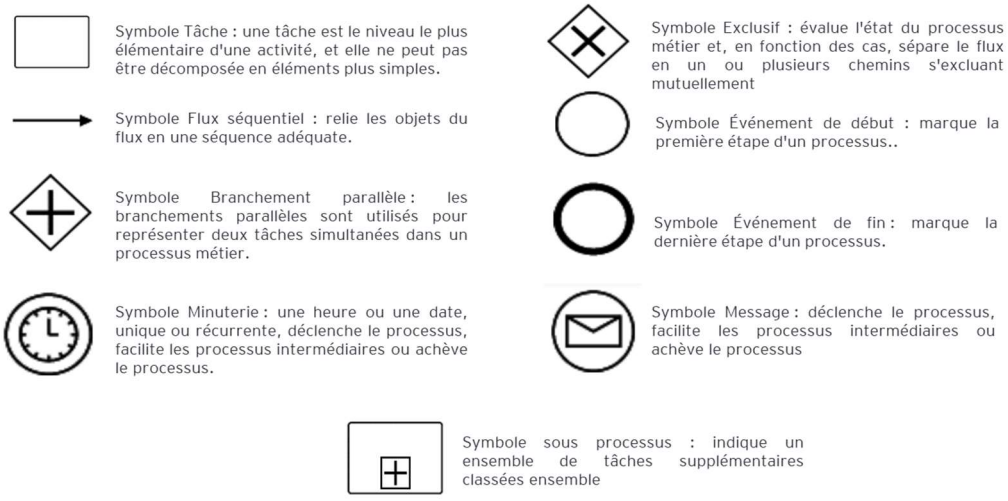


Figure 2 : Légende BPMN 2.0

1.2 Rappel des acteurs du Système d'identification cible

Lors du livrable L9, trois groupes d'acteurs intervenant dans la solution cible ont été identifiés. Chaque groupe peut être constitué par un ou plusieurs acteurs. Les groupes identifiés sont :

- **Les utilisateurs finaux :** les citoyens, résidents, etc.
- **Les partenaires** : Nous distinguons deux types de partenaires. Les premiers sont les partenaires qui consomment des services fournis par le système d'identification comme les banques, les assurances, hôpitaux, etc. Les seconds sont les partenaires qui fournissent des services utilisés par le système d'identification comme les partenaires d'authentification.
- **Les gestionnaires internes** : ce sont les personnes qui gèrent le système d'identification dans son ensemble. Ces gestionnaires peuvent être des administrateurs, des superviseurs, des opérateurs, etc.

1.3 Terminologie et cas d'usage

1.3.1 Identités et identifiants

Le citoyen/résident possède une identité unique qui est le NPI :

Un numéro unique national d'identification appelé Numéro personnel d'identification (NPI) est attribué à chaque personne lors de son enregistrement au RNPP. Ce numéro est unique, inintelligible et non répétitif. Il est attribué à vie.

Le citoyen/résident, une fois enregistré, lui sera délivré les identifiants suivants :

- **Identifiant physique :** carte NPI/fID

C'est une carte avec deux codes QR sécurisés assurant une sécurité via les tokens JWT[1] signée par la PKI nationale dans le code QR du verso.

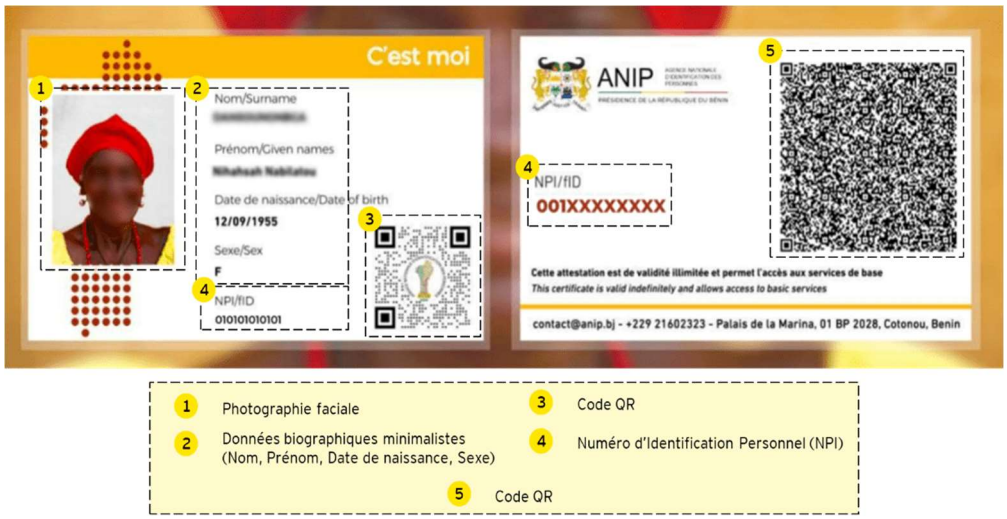


Figure 3: Eléments de la carte NPI/FID

- **Identifiant électronique :**

Mobile ID (QR code du Certificat FID) synchronisé avec le système fID. Le Mobile ID permettra aux citoyens/résidents de s'authentifier en personne en utilisant leur smartphone comme une forme de preuve d'identité électronique.

Le Mobile ID permettra aussi de signer numériquement des documents, des contrats, des formulaires électroniques, etc et de partager certaines informations avec des tiers, tout en ayant un contrôle sur les données qu'ils partagent.

[1] Les « JSON Web Token » ou JWT sont des jetons générés par un serveur lors de l'authentification d'un utilisateur sur une application Web, et qui sont ensuite transmis au client.

- **Identifiant virtuel** :

L'IDV est un numéro aléatoire temporaire et révocable composé de 12 chiffres et associé au numéro NPI. L'IDV peut être utilisé à la place du numéro NPI chaque fois que des services d'authentification ou d'e-KYC sont effectués. L'authentification peut être effectuée en utilisant l'IDV de manière similaire à l'utilisation du NPI. Il n'est pas possible de déduire le numéro NPI à partir du IDV. L'IDV ne peut être généré que par le titulaire du NPI.

Il est possible de remplacer l'IDV déjà crée par un nouveau IDV ou de le révoquer. Ces options seront disponibles via le portail fID, et l'application mobile.

Le choix de la durée de l'IDV et de sa génération automatique ou pas implique des aspects technologiques (impact sur le SI et l'architecture), réglementaires (conformité avec la législation béninoise) et stratégiques (être en ligne avec les décisions politiques) qu'il faut prendre en compte. Ainsi la décision de permettre à la solution d'identification de créer un nouveau numéro (i.e. IDV) en plus de l'existant (i.e. NPI) devra donc être acté au moment opportun par les parties prenantes locales.

1.3.2 Cas d'usage

Deux cas d'usage sont possibles et sont les suivants :

- **Citoyen/résident hors ligne :**

Le citoyen se déplace vers le fournisseur de service physiquement pour s'authentifier via 3 alternatives :

1. Si le citoyen dispose de sa carte physique fID : il s'authentifie moyennant cette carte grâce au QR code avec un autre facteur (Biométrie ou OTP)
2. Si le citoyen dispose de sa carte électronique fID, Il la présente au fournisseur de service qui va vérifier le QR code grâce à l'application de vérification des identités et l'authentifier si vérification avec succès accompagné d'un autre facteur (Biométrie ou PIN)
3. SI le citoyen ne dispose pas de sa carte physique ni de sa carte électronique, uniquement de son Numéro NPI ou IDV, il s'authentifie moyennant les modalités suivantes qui sont détaillées par la suite :
    - Authentification biométrique
    - Authentification e-KYC

- **Citoyen/résident en ligne :**

Le citoyen a accès à une connexion Internet et souhaite bénéficier d'un service auprès des fournisseurs de service moyennant les canaux suivants :

Canal 1 : le portail fID

Portail web sur laquelle le citoyen créé un compte et s'authentifie moyennant les modalités suivantes :

- Authentification en ligne OTP
- Authentification par mot de passe

Canal 2 : Application mobile

Application mobile sur laquelle le citoyen crée un compte et s'authentifie moyennant les modalités suivantes

- Authentification PIN
- Authentification par mot de passe

Les deux canaux donnent la possibilité au citoyen de gérer son identité à savoir :

- Révocation IDV
- Révocation mobile ID
- Edition/Réédition certification fID
- Mise à jour des données d'identification démographiques
- Mise à jour des données biométriques
- Verrouillage/déverrouillage du NPI
- Gestion du profil et suivi des mises à jour

2 Processus d'enregistrement

2. Processus d'enregistrement

Afin de pouvoir disposer de son NPI unique qui lui permet d'utiliser les services liés à la gestion d'identité, il est d'abord nécessaire que le citoyen/résident soit enregistré au préalable dans la base de données de la solution d'identification (RNPP).

Le processus d'enregistrement des citoyens/résidents permet d'assurer l'acquisition des données nécessaires comme : les données démographiques, biométriques (empreintes, portrait), la signature, et les pièces jointes. Et il est couronné - après la vérification des informations d'enregistrement – par la génération d'un numéro NPI/fID.

2.1 Processus de pré-enregistrement

2.1.1 Création d'un rendez-vous

Afin de fluidifier l'enregistrement en question, un processus de pré-enregistrement peut être instauré, ce qui permet notamment à l'agent d'enregistrement d'avoir en amont un ensemble d'informations qui ne seront pas ressaisies à l'enregistrement.

Le processus de pré-enregistrement encapsule l'ensemble des activités nécessaires pour demander un rendez-vous et gérer ce rendez-vous d'enregistrement, dont essentiellement le sous processus de création d'un rendez-vous, illustré par la figure ci-dessous.

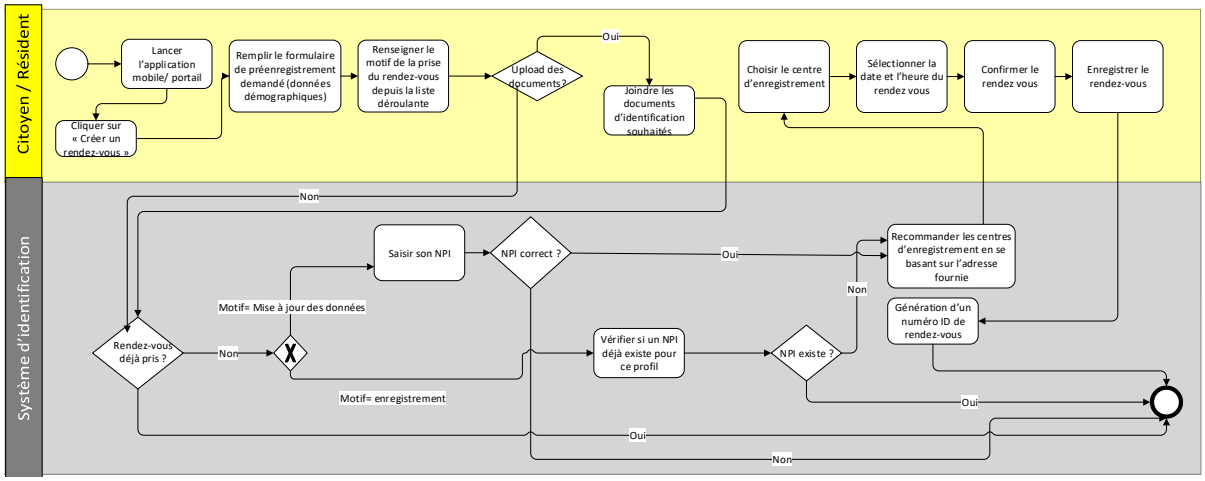


Figure 4 : Processus de création d'un rendez vous

Ce sous-processus explique les étapes à suivre par un citoyen/résident pour prendre rendez-vous afin de procéder à son enregistrement. Lorsqu'il lance son application mobile ou le portail fID, le citoyen/résident clique sur "créer un rendez-vous" et remplira le formulaire en fournissant certaines informations demandées comme ses données démographiques et son adresse mail.

Le citoyen/résident doit renseigner le motif de la prise de rendez-vous en choisissant parmi ces deux options : faire l'enregistrement ou mettre à jour ses données démographiques ou biométriques. Le motif sélectionné permettra d'afficher la liste de documents requis. Par la suite, le citoyen/résident aura la possibilité de choisir l'option d'uploader des documents à travers laquelle il a la possibilité de charger ses

documents d'identification et ceci afin de gagner du temps lors du processus de l'enregistrement ou de mise à jour des données.

Le système vérifiera ensuite si un rendez-vous a déjà été pris pour ce citoyen/résident, en se basant sur l'adresse e-mail fournie dans le formulaire. Si aucun rendez-vous n'a encore été pris, le système vérifiera par la suite selon le motif choisi la validité de sa demande, si le motif choisi est l'enregistrement alors qu'un NPI existe déjà pour ce citoyen dans la base de données la demande sera rejetée.

Si le motif est la mise à jour des données et que le citoyen/résident saisit un NPI qui ne correspond pas aux données saisies dans le formulaire le système rejettera la demande également.

Dans le cas où la demande est acceptée, le système recommandera un centre d'enregistrement en fonction de l'adresse fournie (commune/arrondissement) par le citoyen/résident sur le territoire. Une fois que le centre est choisi, l'utilisateur sélectionnera la date et l'heure de son rendez-vous. Après confirmation, le citoyen/résident recevra un numéro ID unique qu'il utilisera lors de son enregistrement. Les étapes constitutives du processus de création ou de mise à jour d'un rendez-vous sont détaillées dans le tableau suivant.

Etape	Responsable/Système	Description
Lancer l'application mobile/ portail	Citoyen /Résident	Le citoyen/résident lance le portail fID ou l'application mobil e
Cliquer sur « créer un rendez-vous »	Citoyen /Résident	Le citoyen/résident choisit le champ présent dans le portail ou l'application mobile « créer un rendez-vous »
Remplir le formulaire de préenregistrement demandé	Citoyen /Résident	Le citoyen/résident sera amené à remplir les champs demandés afin de créer un rendez-vous en spécifiant son adresse mail
Renseigner le motif de la prise du rendez-vous	Citoyen /Résident	Le citoyen/résident peut prendre un rendez-vous soit pour faire l'enregistrement soit pour mettre à jour ses données biométriques ou démographiques
Choisir d'uploader des documents d'identification	Citoyen /Résident	Le citoyen/résident peut charger des documents d'identification qui seront utilisées par la suite lors du processus d'enregistrement ou de mise à jour des données (cette étape est facultative)
Rendez-vous existe déjà	Système d'identification	Le système doit vérifier si un rendez-vous déjà existe pour ce citoyen/résident ou pas en se basant sur l'adresse mail fourni dans le formulaire de préenregistrement
Selon le motif du rendez-vous, le système d'identification vérifie la légitimité de la demande	Système d'identification	• Si le motif est l'enregistrement, le système vérifier qu'aucun NPI est attribué au demandeur du rendez-vous en se basant sur les données démographiques remplies dans le formulaire, si un NPI existe déjà, la demande de prise de rendez-vous est rejetée. • Si le motif est la mise à jour des données, le citoyen/résident doit saisir son NPI, le système vérifiera si ce NPI correspond aux données saisies dans le formulaire, si le NPI

Etape	Responsable/Système	Description
		ne correspond pas la demande de prise de rendez-vous est rejetée.
Recommander les centres d'enregistrement	Système d'identification	Si la demande de prise de rendez-vous est acceptée, le système d'identification propose une liste des centres d'enregistrement les plus proches du citoyen/résident selon l'adresse fourni et la résidence (commune/arrondissement).
Choisir le centre d'enregistrement	Citoyen /Résident	Le citoyen/résident choisit le centre d'enregistrement qui lui convient le mieux parmi la liste des centres proposée par le système.
Sélectionner la date et l'heure du rendez vous	Citoyen /Résident	Le citoyen/résident sélectionne la date et l'heure du rendez-vous qui lui conviennent en fonction des créneaux disponibles sur la plateforme.
Confirmer le rendez vous	Citoyen /Résident	Le citoyen/résident confirme son rendez-vous
Générer un numéro ID de rendez-vous	Système d'identification	Le système génère un numéro ID unique du rendez-vous pris pour l'enregistrement

Tableau 4 : Tableau descriptif du processus de création et de mise à jour d'un rendez-vous

2.1.2 Mise à jour d'un rendez-vous

En cas de besoin, le citoyen/résident doit mettre à jour son rendez-vous de pré-enregistrement en suivant le processus « Mise à jour d'un rendez-vous » illustré par la figure ci-dessous.

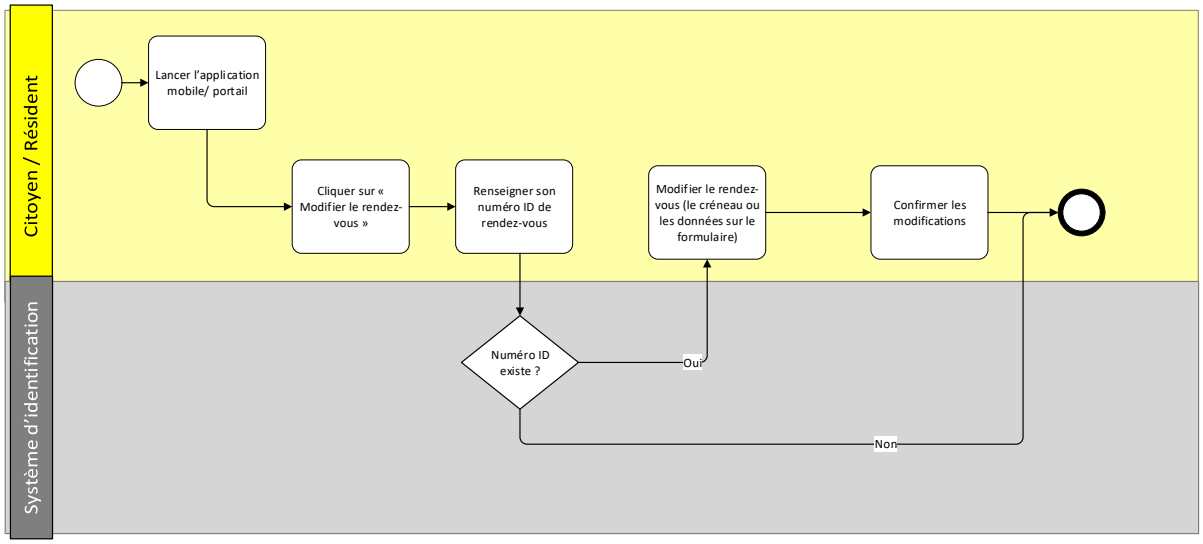


Figure 5 : Processus mettre à jour un rendez-vous

Le citoyen ou résident commence par ouvrir l'application mobile ou le portail fID, puis sélectionne l'option "Modifier le rendez-vous". Ensuite, il doit fournir le numéro ID du rendez-vous. Le système effectuera une vérification pour déterminer si un numéro ID correspondant existe dans la base de données. Si tel est le cas, le citoyen pourra accéder à son rendez-vous et le modifier selon ses besoins.

A noter qu'en cas de contrainte de la part de l'ANIP le citoyen sera informé par mail et par SMS de cette contrainte et sera invité à modifier / annuler son rendez-vous dans un délai bien défini, au-delà ce délai, le rendez-vous sera supprimé automatiquement

Le tableau suivant reprend les principales étapes du processus mentionné.

Etape	Responsable/Système	Description
Lancer l'application mobile/ portail	Citoyen /Résident	Le citoyen/résident lance son application mobile ou sur le portail fID.
Cliquer sur « modifier le rendez-vous »	Citoyen /Résident	Le citoyen/résident choisit l'option de modification du rendez-vous
Renseigner le numéro ID de rendez-vous fourni	Citoyen /Résident	Le citoyen/résident renseigne le numéro ID du rendez-vous afin de pouvoir le modifier
Rendez-vous existe déjà	Système d'identification	Le système doit vérifier si un rendez-vous existe déjà pour ce citoyen/résident ou pas selon le numéro ID fourni
Si Oui modifier le rendez vous	Citoyen /Résident	Le citoyen/résident met à jour son rendez-vous
Modifier le rendez-vous	Citoyen /Résident	Le citoyen/résident modifie son rendez-vous en modifiant soit le créneau soit les données démographiques sur le formulaire
Confirmer les modifications	Citoyen /Résident	Le citoyen/résident confirme son choix de modification

Tableau 5 : Tableau descriptif du processus de la mise à jour d'un rendez-vous

2.1.3 Annulation d'un rendez-vous

Toujours dans une démarche de facilitation et de simplification des démarches d'enregistrement pour le citoyen/résident, il est important de laisser une marge de liberté permettant d'offrir une option d'annulation du rendez-vous d'enregistrement, avec la possibilité de revenir en créer un nouveau à la date et heure souhaitées. Le schéma ci-dessous modélise les étapes clés dans le sous-processus de suppression d'un rendez-vous.

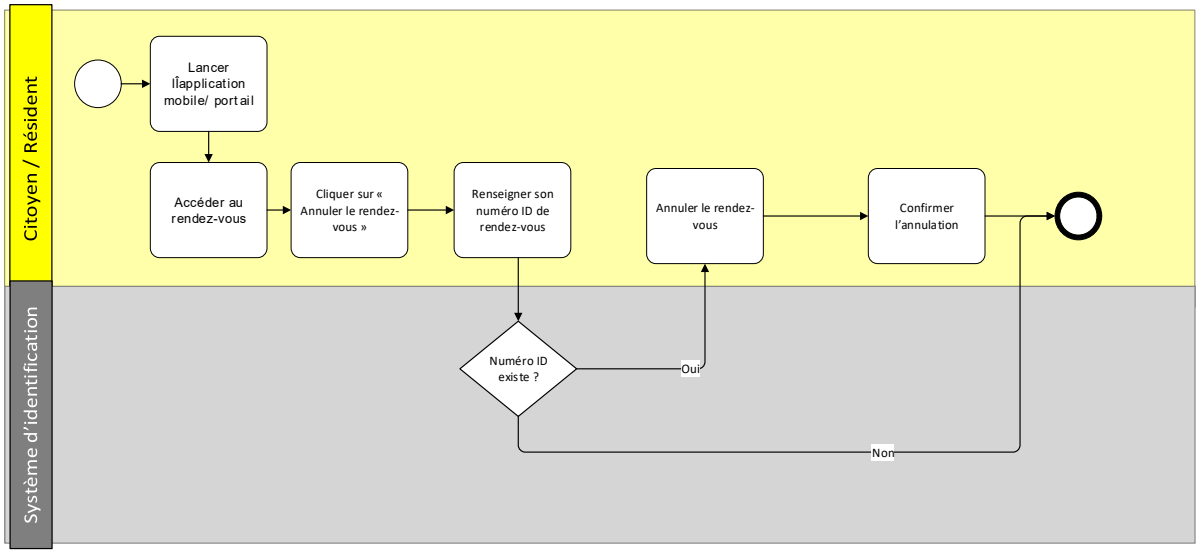


Figure 6 : Processus d'annulation d'un rendez-vous

Le citoyen ou résident commence par ouvrir l'application mobile ou le portail fID, puis sélectionne l'option "Annuler le rendez-vous". Ensuite, il doit fournir le numéro ID du rendez-vous. Le système effectuera une vérification pour déterminer si un numéro ID correspondant existe dans la base de données. Si tel est le cas, le citoyen pourra accéder à son rendez-vous et le supprimer.

A noter qu'en cas de contrainte de la part de l'ANIP le citoyen sera informé par mail et par SMS de cette contrainte et sera invité à modifier / annuler son rendez-vous dans un délai bien défini, au-delà ce délai, le rendez-vous sera supprimé automatiquement. Même en cas de suppression, il doit être possible de tracer les demandes de rendez-vous.

Le tableau suivant reprend les principales étapes de sous processus de l'annulation du rendez-vous.

Etape	Responsable/Système	Description
Lancer l'application mobile/ portail	Citoyen /Résident	Le citoyen/résident lance son application mobile ou sur le portail fID.
Choisir l'option « annuler un rendez-vous »	Citoyen /Résident	Le citoyen/résident choisit l'option d'annulation du rendez-vous
Renseigner le numéro ID du rendez-vous fourni	Citoyen /Résident	Le citoyen/résident renseigne le numéro ID du rendez-vous afin de pouvoir l'annuler
Rendez-vous existe déjà	Système d'identification	Le système doit vérifier si un rendez-vous existe déjà pour ce citoyen/résident ou pas selon le numéro ID fourni
Si Oui accéder au rendez vous	Citoyen /Résident	Le citoyen/résident accède à son rendez-vous
Annuler le rendez-vous	Citoyen /Résident	Le citoyen/résident Annule son rendez-vous
Confirmer l'annulation du rendez-vous	Citoyen /Résident	Le citoyen/résident confirme son choix d'annulation

Tableau 6 : Tableau descriptif du processus d'annulation de rendez-vous

2.2 Processus d'enregistrement et importation des dossiers

La phase de l'enregistrement constitue une étape très importante dans le sens où c'est l'étape qui va aboutir à la génération effective du NPI. Cette étape peut être précédée d'une phase de préenregistrement, toutefois il demeure possible pour le citoyen/résident de procéder à l'enregistrement sans passer par l'étape pré-enregistrement.

La phase de l'enregistrement du citoyen/résident implique une présence physique du citoyen/résident dans un centre d'enregistrement, l'opérateur commence par vérifier l'âge du citoyen :

- **Si le citoyen/résident a un âge < 5 ans**

La première étape pour enregistrer un nouveau-né dans le système d'identification national au Bénin est d'effectuer une déclaration de naissance. Un formulaire est rempli par l'agent accoucheur si le nouveau-né est né dans un établissement de santé. La déclaration électronique du nouveau-né est faite aussi par le service téléphonique USSD dédié.

Si le nouveau-né est né en dehors d'un service de santé, un agent du service d'état civil qui se trouve dans le service de santé le plus proche ou dans le centre d'état civil adéquat remplit le formulaire.

Les parents/tuteur légal du nouveau-né doivent se présenter au centre d'enregistrement avec les informations nécessaires, telles que l'identité des parents, les pièces de déclaration de naissance, l'acte de mariage des parents ou l'acte de reconnaissance de paternité. Les agents du centre d'enregistrement utiliseront ensuite le système d'identification pour créer un profil pour le nouveau-né et lui attribuer un numéro d'identification unique. Les parents recevront une copie de ce profil et le nouveau-né sera officiellement enregistré dans le système d'identification.

Cependant, il est important de noter qu'il devra être enregistré avec des données biométriques fiables dès que possible pour assurer une identification précise et sûre. Les données biométriques, telles que les empreintes digitales ou les photographies du visage, peuvent être collectées plus tard lorsque l'enfant est plus âgé et capable de le faire. Les parents peuvent ainsi retourner au centre d'enregistrement avec l'enfant entre l'âge de 5 et 18 ans. Les données biométriques (les empreintes digitales et les données faciales) seront collectées et stockées dans la base de données RNPP.

La figure ci-dessous décrit le processus d'enregistrement détaillé pour les enfants ayant un âge inférieur à 5 ans.

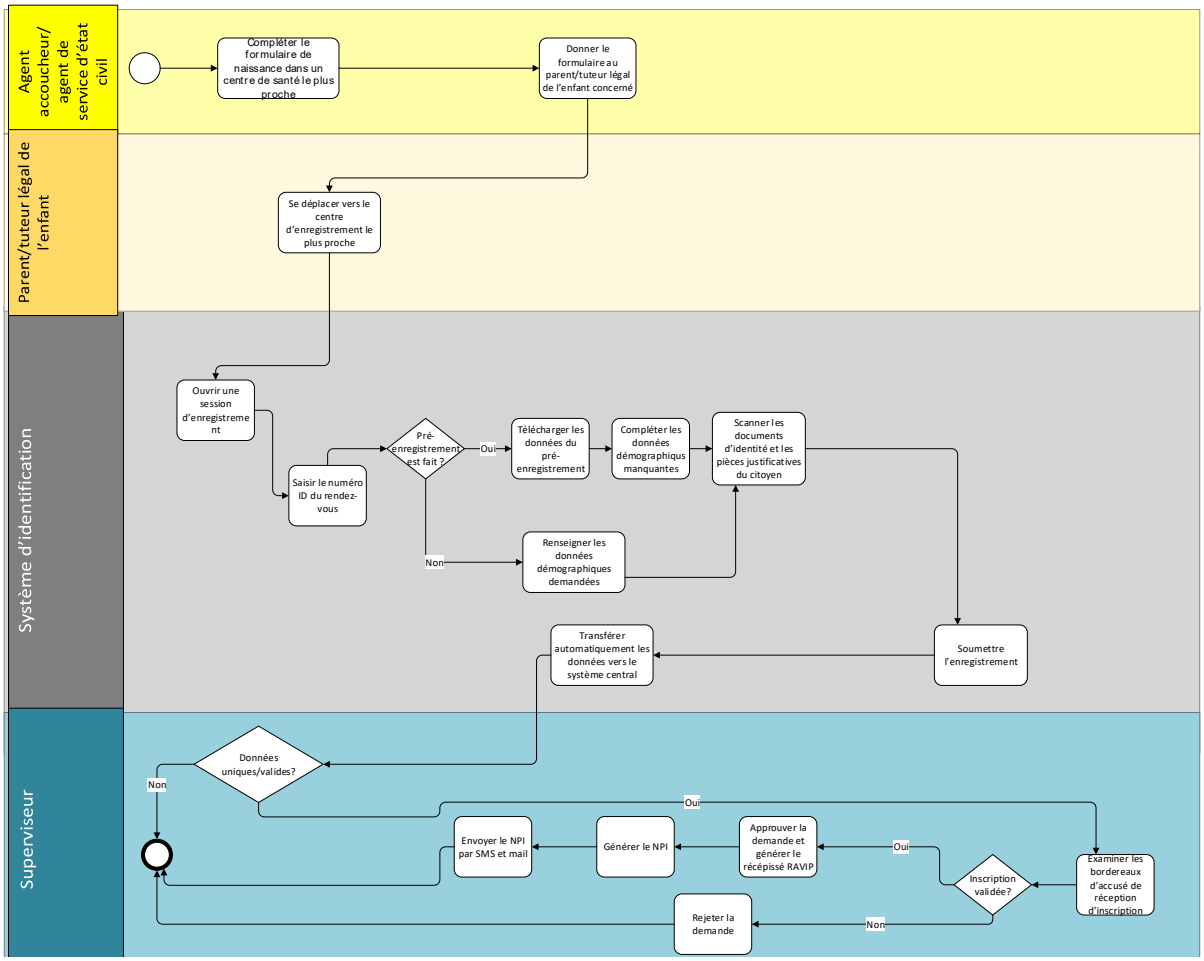


Figure 7 : Processus d'enregistrement des citoyens ayant un âge < 5 ans

ci-dessous le tableau qui décrit l'ensemble de ces étapes

Etape	Responsable/Système	Description
Compléter le formulaire dans un centre de santé le plus proche	Agent accoucheur / agent de service d'état civil	L'agent accoucheur ou l'agent de service d'état civil remplit un formulaire de la naissance dans le centre de santé le plus proche
Donner le formulaire de la naissance au parent/tuteur légal	Agent accoucheur / agent de service d'état civil	L'agent accoucheur ou l'agent de service d'état civil donne le formulaire de naissance au parent ou tuteur légal du nouveau-né
Se rendre au centre d'enregistrement choisi.	Parent/tuteur légal	Le citoyen/Résident se rend au centre d'enregistrement choisi.
Ouvrir une session d'enregistrement	L'opérateur d'enregistrement	L'opérateur d'enregistrement démarre une session d'enregistrement pour le citoyen/résident.
Saisir le numéro ID	L'opérateur d'enregistrement	L'opérateur saisit le numéro ID du rendez-vous du citoyen/résident
Vérifier si un pré-enregistrement a déjà été réalisé ?	L'opérateur d'enregistrement	L'opérateur d'enregistrement doit vérifier si le citoyen/résident a fait un pré-enregistrement ou pas

Etape	Responsable/Système	Description
Option 1 : sans préenregistrement Renseigner les données demandées	L'opérateur d'enregistrement	Selon la situation (le citoyen/résident n'a pas fait de préenregistrement), l'opérateur renseigne les données requises en totalité.
Option 2 : avec préenregistrement Télécharger les données préremplies puis les compléter.	L'opérateur d'enregistrement	Selon la situation (le citoyen/résident a déjà fait un préenregistrement), l'opérateur complète la saisie des données requises.
Scanner les documents d'identité du citoyen.	L'opérateur d'enregistrement	L'opérateur scanne les documents d'identité du citoyen/résident nécessaires pour l'enregistrement.
Soumettre l'enregistrement.	L'opérateur d'enregistrement	L'opérateur soumet la demande d'enregistrement du citoyen/résident.
Transférer automatiquement les données vers le système central	L'opérateur d'enregistrement	Les données sont transférées automatiquement vers le système central
Vérifier l'unicité des données saisies	Système d'identification	Le système vérifie grâce à des contrôles de dédoublonnage que les données saisies sont uniques
Examiner les bordereaux d'accusé de réception d'inscription	Superviseur	Le superviseur examine les bordereaux d'accusé de réception d'inscription
Inscription valide ?	Superviseur	Le superviseur doit vérifier si l'inscription du citoyen/résident est valide ou pas
Approuver la demande et générer un récépissé RAVIP	Superviseur	Le superviseur accepte la demande d'enregistrement du citoyen/résident si la demande est valide et lui génère un récépissé RAVIP
Rejeter la demande	Superviseur	Le superviseur rejette la demande d'enregistrement du citoyen/résident si la demande n'est pas valide.
Générer le NPI	Système d'identification	Si la demande est approuvée, le NPI du citoyen sera généré
Envoyer le NPI	Système d'identification	Le NPI sera envoyé par mail et SMS au citoyen

Tableau 7 : Tableau décrivant le process d'enregistrement des citoyens ayant un âge <5 ans

- **Si le citoyen/résident a un âge > = 5 ans**

Ce dernier doit présenter à l'opérateur d'enregistrement les documents d'identité nécessaires pour l'enregistrement et aussi fournir les données biométriques requises. L'opérateur renseigne les champs relatifs aux données démographiques et scanne les documents faisant office de preuve d'identité. Il passe après à la prise des données biométriques et soumet l'enregistrement.

Ce processus impliquera aussi une intervention du superviseur qui aura la tâche d'examiner et de valider les demandes d'inscription.

Une fois le citoyen enregistré il lui sera généré un numéro NPI en plus du récépissé RAVIP.

Il est important de noter que les données biométriques doivent être régulièrement mises à jour pour refléter les changements dans la situation de la personne. Les fréquences de mise à jour régulière peuvent varier, mais pour les données démographiques et biométriques, il est recommandé de le faire tous les 10 ans.

La figure ci-dessous présente une modélisation détaillant le processus d'enregistrement et d'importation du dossier du citoyen/résident ayant un âge > = 5 ans

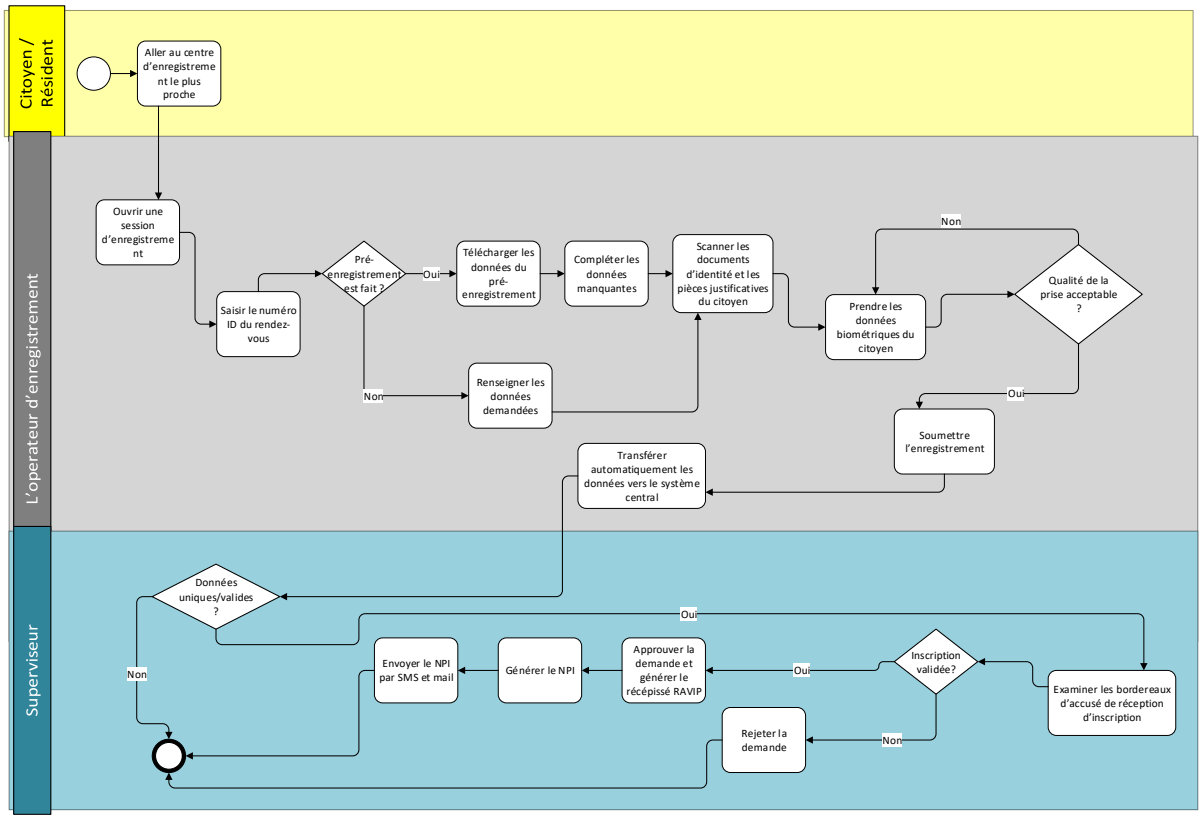


Figure 8 : Processus d'enregistrement des citoyens ayant un âge >= 5 ans

Les différentes étapes composant ce processus sont décrites dans le tableau qui suit.

Etape	Responsable	Description
Se rendre au centre d'enregistrement choisi.	Citoyen / Résident	Le citoyen/Résident se rend au centre d'enregistrement choisi.
Ouvrir une session d'enregistrement	L'opérateur d'enregistrement	L'opérateur d'enregistrement démarre une session d'enregistrement pour le citoyen/résident.
Saisir le numéro ID	L'opérateur d'enregistrement	L'opérateur saisit le numéro ID du rendez-vous du citoyen/résident
Vérifier si un pré-enregistrement a déjà été réalisé ?	L'opérateur d'enregistrement	L'opérateur d'enregistrement doit vérifier si le citoyen/résident a fait un pré-enregistrement ou pas

Etape	Responsable	Description
Option 1 : sans préenregistrement Renseigner les données demandées	L'opérateur d'enregistrement	Selon la situation (le citoyen/résident n'a pas fait de préenregistrement), l'opérateur renseigne les données requises en totalité.
Option 2 : avec préenregistrement Télécharger les données préremplies puis les compléter.	L'opérateur d'enregistrement	Selon la situation (le citoyen/résident a déjà fait un préenregistrement), l'opérateur complète la saisie des données requises.
Scanner les documents d'identité du citoyen.	L'opérateur d'enregistrement	L'opérateur scanne les documents d'identité du citoyen/résident nécessaires pour l'enregistrement.
Prendre les données biométriques du citoyen.	L'opérateur d'enregistrement	L'opérateur prend les données biométriques du citoyen nécessaires pour l'enregistrement.
Vérifier que les données biométriques sont à la qualité requise.	L'opérateur d'enregistrement	L'opérateur d'enregistrement doit vérifier la qualité des données biométriques prises avant de poursuivre vers la prochaine étape
Soumettre l'enregistrement.	L'opérateur d'enregistrement	L'opérateur soumet la demande d'enregistrement du citoyen/résident.
Transférer automatiquement les données vers le système central	L'opérateur d'enregistrement	Les données sont transférées automatiquement vers le système central
Vérifier l'unicité des données saisies	Système d'identification	Le système vérifie grâce à des contrôles de dédoublonnage que les données saisies sont uniques
Examiner les bordereaux d'accusé de réception d'inscription	Superviseur	Le superviseur examine les bordereaux d'accusé de réception d'inscription
Inscription valide ?	Superviseur	Le superviseur doit vérifier si l'inscription du citoyen/résident est valide ou pas
Approuver la demande et générer un récépissé RAVIP	Superviseur	Le superviseur accepte la demande d'enregistrement du citoyen/résident si la demande est valide et lui génère un récépissé RAVIP
Rejeter la demande	Superviseur	Le superviseur rejette la demande d'enregistrement du citoyen/résident si la demande n'est pas valide.
Générer le NPI	Système d'identification	Si la demande est approuvée, le NPI du citoyen sera généré
Envoyer le NPI	Système d'identification	Le NPI sera envoyé par mail et SMS au citoyen

Tableau 8 : Tableau descriptif du processus d'enregistrement pour les citoyens ayant un âge >= 5 ans

NB : Il est important de noter que le système met en œuvre une méthode d'adjudication manuelle dans les cas où il existe des soupçons de doublons. Cette fonctionnalité s'avère également être un outil essentiel dans l'exercice continu de l'assurance qualité, exemple de méthode d'adjudication est l'adjudication biométrique manuelle qui aide à la vérification humaine 1:1 et aux contrôles de qualité selon les modalités, pour chaque ensemble de dossiers de personnes identifiés comme correspondant par le système ABIS.

3 Processus de création de compte et login

3. Processus de création de compte et login

Afin de bénéficier des services de gestion d'identité et de certains services d'authentification, le citoyen/résident doit créer un compte, en ayant encore une fois le choix de le faire à travers le portail fID ou dans l'application mobile. Dans les sous-sections suivantes, nous allons exposer les processus de création de compte ainsi que les processus de login et cela respectivement pour l'application mobile et pour le portail fID. Ces sous-processus ne peuvent être effectués sans un enregistrement au préalable, car le NPI est nécessaire.

3.1 Saisie et vérification du NPI

Le sous processus « Saisie et vérification du NPI » a pour but de valider que le NPI existe dans le RNPP, si le NPI n'est pas correct au bout de la 3ème tentative, le service sera bloqué pour 24 heures dans la 4ème tentative.

Le graphique suivant expose les étapes qui compose ce processus.

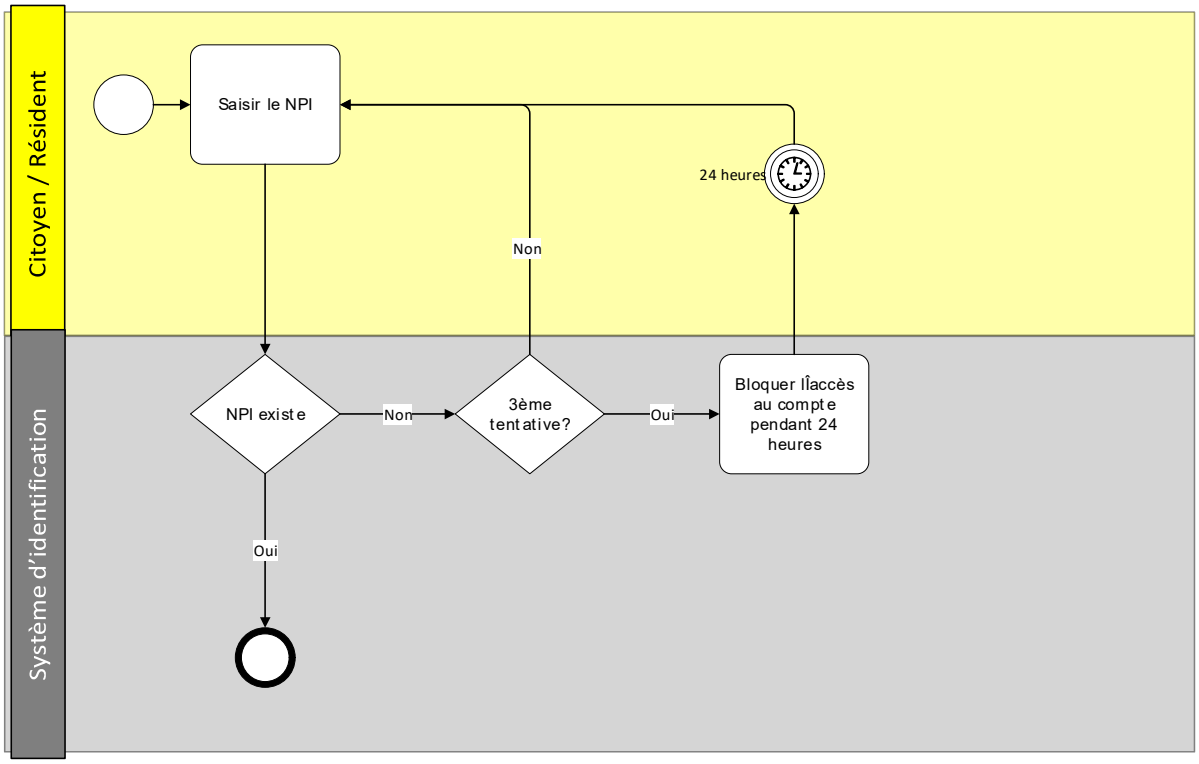


Figure 9 : Processus de saie et de vérification du NPI

Ci-dessous le tableau descriptif de l'ensemble des étapes du processus.

Etape	Responsable/Système	Description
Saisir le NPI	Citoyen /Résident	Après le lancement de l'application, le citoyen/résident doit saisir son NPI dans le champ correspondant
NPI existe ?	Système d'identification	Le système d'identification Vérifiera si ce numéro existe ou pas.

Etape	Responsable/Système	Description
		Si le NPI est introuvable, le citoyen sera amené de nouveau à la page de saisi du NPI, sinon l'étape suivante sera déclenchée.
Bloquer l'accès au compte pendant 24 heures	Système d'identification	Si le NPI n'est pas correct au bout de la 3ème tentative, le service sera bloqué pour 24 heures dans la 4ème tentative.

Tableau 9 : Tableau descriptif du sous processus saisie et validation du NPI

3.2 Création de compte application mobile

La création d'un compte via l'application mobile est une opération que le citoyen/résident peut faire en ligne. En effet le citoyen/résident aura à s'identifier par un code OTP, un mot de passe et un code PIN, auxquels est associée la prise d'une photo du visage après consentement du citoyen/résident, cette photo sera comparée à l'image déjà stockée correspondante au NPI saisi (vérification 1 :1).

Si la vérification est réalisée avec succès le compte est activé.

Le graphique suivant expose les étapes qui compose ce processus.

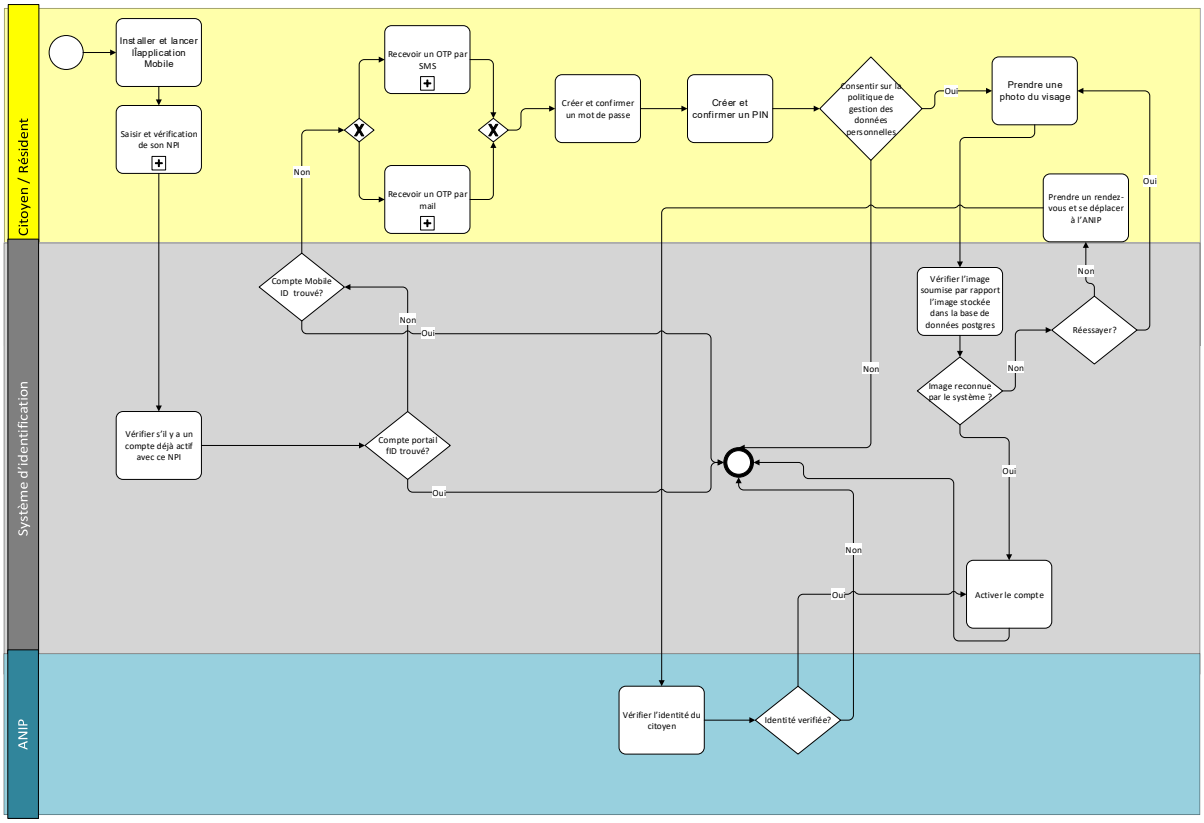


Figure 10 : Processus de création d'un compte application mobile

Ci-dessous le tableau descriptif de l'ensemble des étapes du processus.

Etape	Responsable/Système	Description
Installer et lancer l'application « Mobile ID Bénin »	Citoyen /Résident	Le citoyen/résident doit télécharger, installer, et lancer l'application « mobile ID Bénin » sur son smartphone.

Etape	Responsable/Système	Description
Saisir et vérifier son NPI	Citoyen /Résident	Après le lancement de l'application, le citoyen/résident doit saisir son NPI dans le champ correspondant. Si le NPI est correct, le système poursuit les étapes suivantes, sinon le citoyen doit ressaisir son NPI
Vérifier s'il y a un compte déjà actif	Système d'identification	Le système d'identification vérifiera s'il y a un compte déjà actif pour le NPI en question
Compte mobile ID trouvé ?	Système d'identification	Si le système d'identification ne trouve pas un compte actif pour le NPI saisi il pourra suivre avec les étapes suivantes. Si un compte existe déjà, le process prend fin
Compte portail fID trouvé ?	Système d'identification	
Cliquer sur « recevoir OTP »	Citoyen /Résident	Si le citoyen n'a pas un compte actif, il clique sur le bouton « Recevoir OTP », en choisissant le canal de réception de l'OTP soit par SMS soit par mail.
Créer et confirmer un mot de passe	Citoyen /Résident	Le citoyen doit créer et confirmer un mot de passe. Le mot de passe doit respecter les règles suivantes : • Une taille minimale de 10 caractères. • Contient au moins une lettre en majuscule • Contient au moins une lettre en minuscule • Contient au moins un chiffre. • Contient au moins un caractère spécial (#, @, *, etc.)
Créer un PIN	Citoyen /Résident	Le citoyen doit créer et confirmer un PIN pour accéder à l'ensemble des services fournis par l'application. Le PIN doit respecter les règles suivantes : • Le PIN est composé de 4 caractères • Tous les caractères sont de type entier
Consentir sur la politique de gestion des données personnelles	Citoyen /Résident	Le citoyen/résident lit et accorde son consentement à la politique de protection des données personnelles. Cette politique doit indiquer clairement les modalités d'utilisation et de partage des données des citoyens en interne et avec les fournisseurs de services.
Prendre une photo du visage.	Citoyen /Résident	Le citoyen/résident suit les instructions pour prendre une photo de son visage de plusieurs côtés : vue de face, vue de gauche, vue de droite.
Vérifier l'image soumise par rapport l'image stockée dans la base de données postgres.	Système d'identification	Le système d'identification traite les images soumises par le citoyen et fait une vérification 1 :1 par rapport l'image du citoyen capturée durant l'enregistrement
Prendre un rendez-vous pour vérifier son identité dans le cas ou son identité	Citoyen /Résident	**Dans le cas d'un échec de vérification de l'identité à distance,** le citoyen doit prendre un rendez-vous pour faire cette vérification auprès l'ANIP.

Etape	Responsable/Système	Description
n'a pas pu être vérifiée en ligne		
Vérifier l'identité de la personne	ANIP / centre de vérification	L'agent de l'ANIP doit vérifier que l'identité de la personne présente est la même sur l'application. L'agent demandera les éléments suivants : • Le numéro du rendez-vous affiché sur l'application Mobile ID Bénin • Le certificat fID du citoyen /résident présent L'agent doit vérifier les conditions suivantes avant d'activer le compte : • Le NPI utilisé doit être le même que celui sur le certificat fID fourni • La photo associée au NPI en question doit correspondre à la personne présente sur site
Activer le compte de l'application mobile	citoyen /résident	Une fois que les conditions de vérification sont satisfaites (à distance ou sur le site de l'ANIP), le profil du citoyen/ résident sera activé par le citoyen/résident

Tableau 10 : Tableau descriptif du processus de création du compte application mobile

3.2.1 Réception OTP par SMS

Le citoyen lors de la création de son compte sur l'application mobile ou sur le portail, il sera amené à demander un OTP pour confirmer son identité.

Cet OTP peut être envoyé par SMS ou par mail, le process suivant traite le cas du SMS en mettant en valeur que le citoyen n'a le droit qu'à 3 OTPs par SMS au maximum pendant la journée et que dépassé ce seuil l'envoi d'OTP sera bloqué pendant 24H.

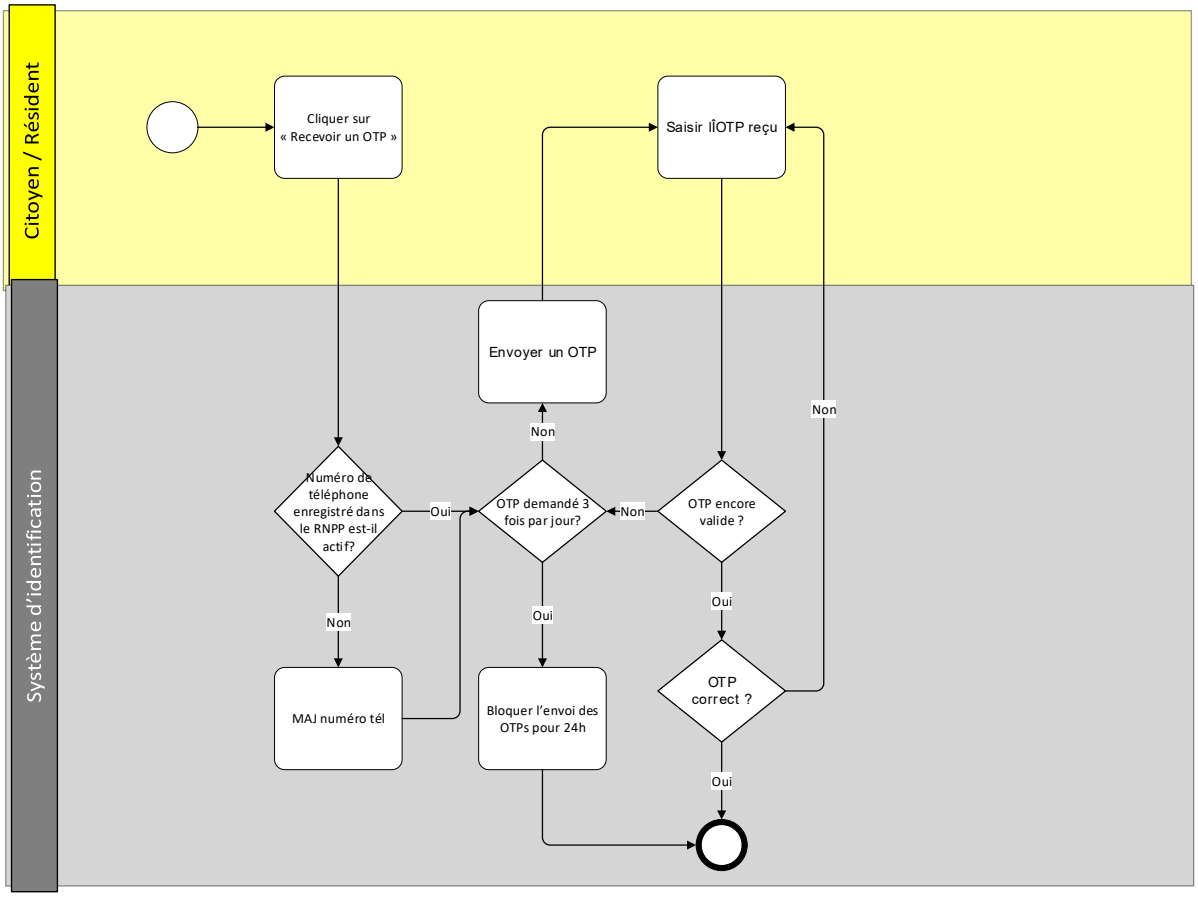


Figure 11 : Processus réception OTP par SMS

Ci-dessous le tableau descriptif de l'ensemble des étapes du processus.

Etape	Responsable/Système	Description
Cliquer sur « recevoir OTP »	Citoyen /Résident	Si le citoyen a déjà un compte, il clique sur le bouton « Recevoir OTP ».
Saisir l'OTP reçu	Citoyen /Résident	Le citoyen/résident saisit l'OTP qu'il a reçu dans un délai qui ne dépasse pas 2 minutes de l'horaire de la demande. Un minuteur sera affiché sur l'écran du smartphone pour indiquer la durée de validité restante pour l'OTP envoyé.
Envoyer un OTP	Système d'identification	Le système générera et enverra l'OTP.
Numéro de téléphone enregistré dans le RNPP est-il actif ?	Système d'identification	Le système d'identification vérifie que le numéro de téléphone enregistré dans le RNPP est actif.
MAJ numéro téléphone	Système d'identification	Si le numéro du téléphone enregistré dans RNPP n'est pas actif, le citoyen/Résident doit mettre à jour son numéro de téléphone
OTP encore valide ?	Système d'identification	Le système d'identification vérifie que l'OTP saisi est encore valide. Cette validité est déterminée en comparant l'horaire de saisie de l'OTP par rapport l'horaire de création de l'OTP
OTP correct ?	Système d'identification	Dans le cas où l'OTP saisi n'est pas correct, un message sera affiché « OTP incorrect » et il doit saisir l'OTP de nouveau.

Etape	Responsable/Système	Description
OTP demandé 3 fois par jour ?	Système d'identification	Le système vérifiera si un OTP a été demandé plus que trois fois par ce NPI
Bloquer l'envoi des OTPs pour 24h	Système d'identification	Dans le cas où le citoyen/résident a demandé 3 OTP durant la même journée, le système bloquera la génération des OTP pendant la prochaine 24h. A la demande du 4ème OTP par le citoyen/résident. Le message suivant sera affiché « Vous avez atteint votre plafond d'OTP par jour, prière d'essayer après 24h »

Tableau 11 : Tableau descriptif du processus réception OTP par SMS

3.2.2 Réception OTP par mail

Le citoyen lors de la création de son compte sur l'application mobile ou sur le portail, il sera amené à demander un OTP pour confirmer son identité.

Contrairement aux SMS, Cet OTP peut être envoyé par mail autant de fois que le citoyen le souhaite sans un seuil prédéfini

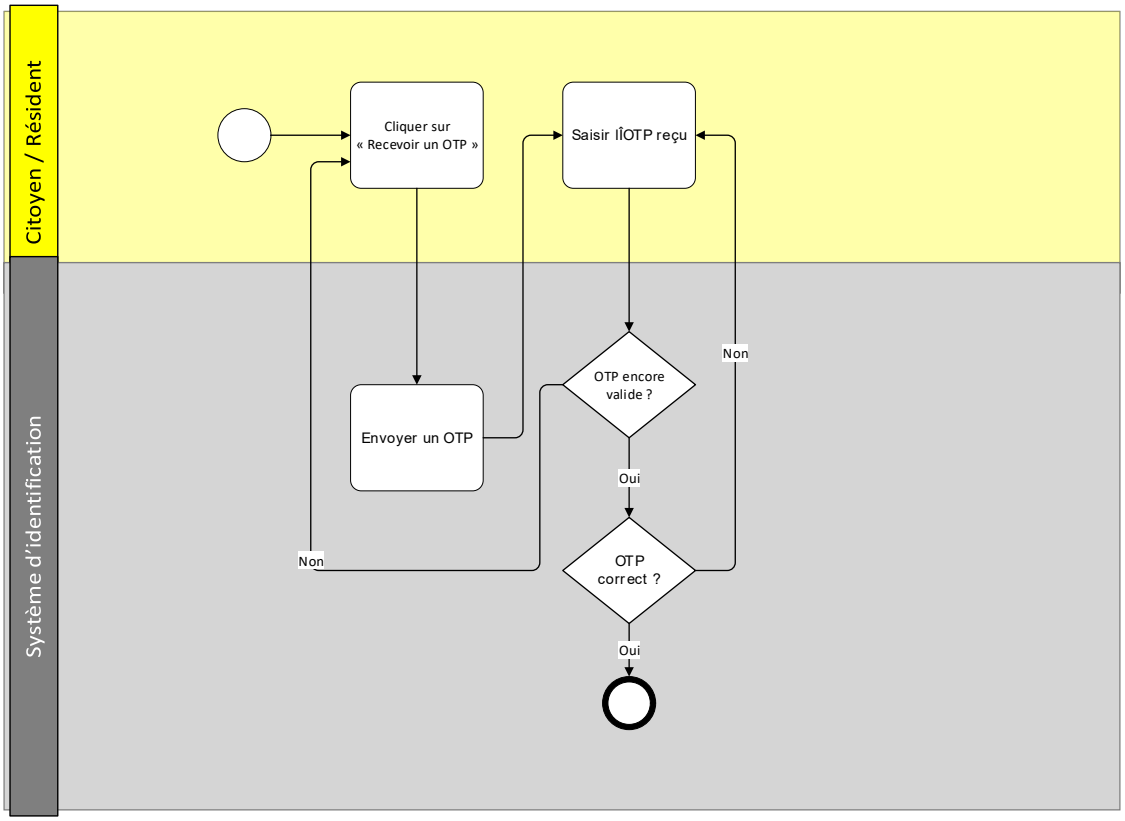


Figure 12 : Processus réception d'OTP par mail

Ci-dessous le tableau descriptif de l'ensemble des étapes du processus.

Etape	Responsable/Système	Description
Cliquer sur « recevoir OTP »	Citoyen /Résident	Si le citoyen a déjà un compte, il clique sur le bouton « Recevoir OTP ».

Etape	Responsable/Système	Description
Saisir l'OTP reçu	Citoyen /Résident	Le citoyen/résident saisit l'OTP qu'il a reçu dans un délai qui ne dépasse pas 2 minutes de l'horaire de la demande. Un minuteur sera affiché sur l'écran du smartphone pour indiquer la durée de validité restante pour l'OTP envoyé.
Envoyer un OTP	Système d'identification	Le système générera et enverra l'OTP.
OTP encore valide ?	Système d'identification	Le système d'identification vérifie que l'OTP saisi est encore valide. Cette validité est déterminée en comparant l'horaire de saisie de l'OTP par rapport l'horaire de création de l'OTP
OTP correct ?	Système d'identification	Dans le cas où l'OTP saisi n'est pas correct, un message sera affiché « OTP incorrect » et il doit saisir l'OTP de nouveau.

Tableau 12 : Tableau descriptif du processus réception OTP par mail

3.3 Login sur l'application mobile

Une fois le compte sur l'application mobile créé, le citoyen/résident aura l'opportunité d'accéder aux différents services, mais avant il doit s'authentifier pour accéder à son compte : c'est le processus login sur l'application mobile, détaillé dans le graphique suivant.

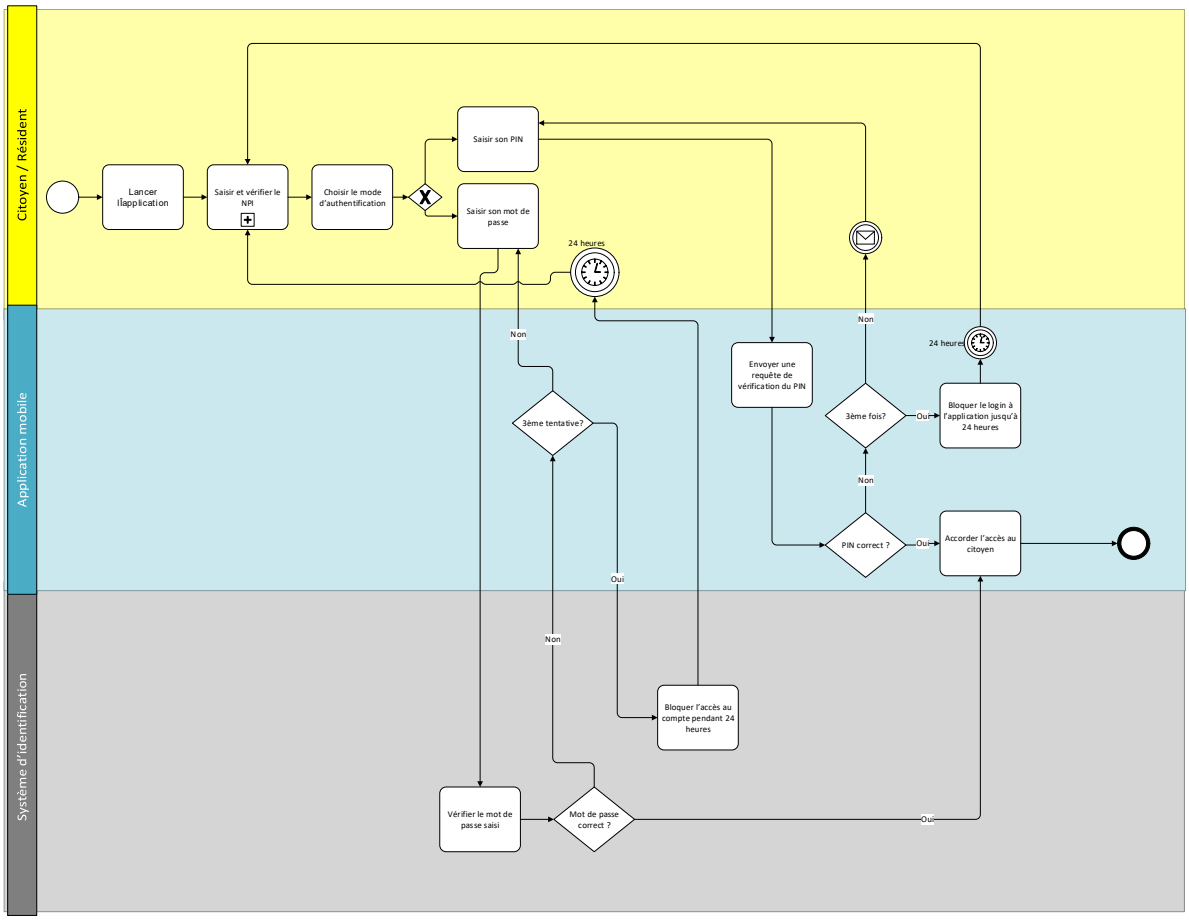


Figure 13 : Processus de login à l'application mobile

Le citoyen/résident aura le choix de s'authentifier par son mot de passe ou par son code PIN. Il est déconnecté systématiquement de l'application après 5 min d'inactivité sur ce compte mais peut se reconnecter au besoin avec son login. L'ensemble des étapes est récapitulé dans le tableau descriptif qui suit.

Etape	Responsable/Système	Description
Lancer l'application	Citoyen / résident	Le citoyen/résident lance l'application installée sur son smartphone.
Saisir son NPI	Citoyen / résident	Le citoyen/résident saisi son NPI et clique sur le bouton « Suivant ».
Envoyer une requête de vérification du NPI	Application mobile ID	L'application mobile envoi une requête de vérification du NPI au moteur de déduplication du système d'identification.
NPI existant ?	Système d'identification	Le système d'identification répondra s'il a trouvé le NPI saisi ou pas. Si le NPI est introuvable, le citoyen sera amené de nouveau à la page de saisi du NPI, sinon l'étape suivante sera déclenchée.
Saisir son PIN	Citoyen / résident	Le citoyen/résident saisit son PIN composé de 4 chiffres.
Envoyer une requête de vérification du PIN	Application mobile ID	L'application mobile ID envoi une requête de vérification du PIN au système d'identification

Etape	Responsable/Système	Description
PIN correct ?	Système d'identification	Le système d'identification vérifiera l'authenticité du PIN saisi par le citoyen/résident. Si le PIN saisi est authentique, l'étape « Accorder l'accès à l'application » sera déclenché.
3ème fois ?	Application mobile	L'application mobile vérifiera si c'est la troisième fois que le PIN est incorrect. Si c'est le cas, l'accès à l'application sera bloqué pendant 24 heures. Sinon le citoyen/résident peut re-saisir son PIN.
Accorder l'accès à l'application	Application mobile	Après la satisfaction des conditions de login, le citoyen/résident aura l'accès à l'application mobile ID et peut se bénéficier des services disponibles.

Tableau 13 : Tableau descriptif du processus de login au mobile ID

3.4 Création de compte portail fID

Le portail fID est une interface WEB dédiés aux citoyens/résidents pour gérer leurs identités qui pourrait être développée en tant qu'une sous-composante du portail actuel de l'ANIP https://eservices.anip.bj/.

Tel qu'illustré par la figure suivante, et comme cela a été le cas avec l'application mobile, le citoyen/résident a aussi la possibilité de créer son compte depuis le portail. Cette opération garantit un même niveau de sécurité et de facilité d'accès tout en s'adaptant aux spécificités d'une utilisation web depuis n'importe quel terminal.

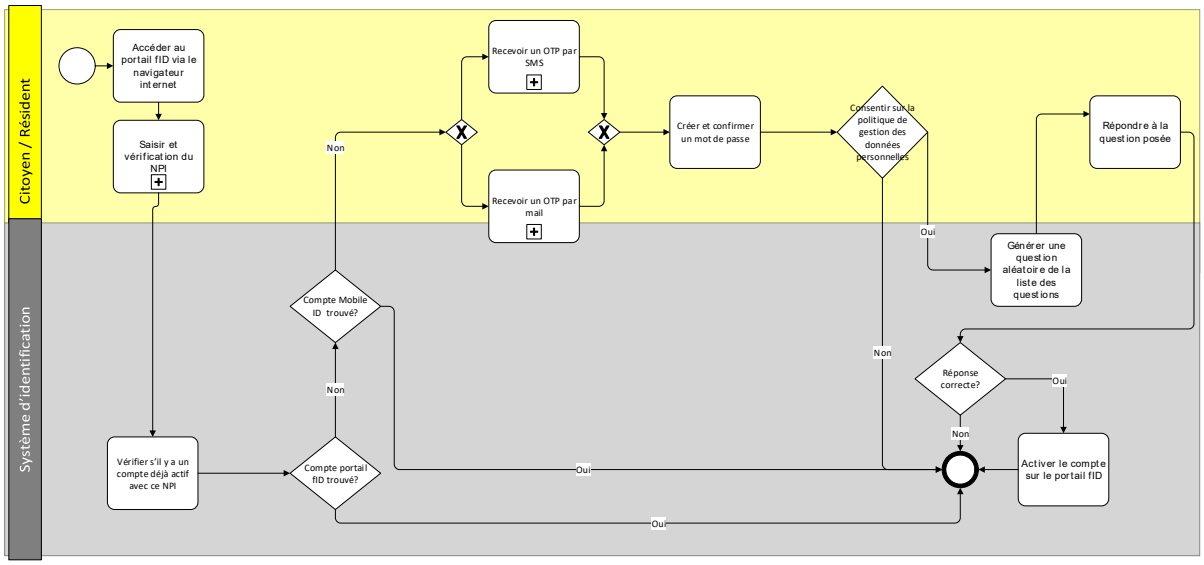


Figure 14 : Processus de création d'un compte portail fID

Lors de la création d'un compte via l'application web sur le portail, le citoyen/résident aura à s'identifier par l'utilisation d'un code OTP, et par un mot de passe, auxquels est associée après le consentement du citoyen/résident la réponse à une question aléatoire portant sur des informations personnelles du citoyen/résident, déjà enregistrée dans la base de données RNPP.

Le tableau suivant expose les étapes qui compose ce processus.

Etape	Responsable/Système	Description
Accéder au portail fID via un navigateur internet	Citoyen /Résident	Le citoyen /résident accède au portail fID en utilisant un navigateur internet de n'importe quel terminal (smartphone, ordinateur, tablette, etc.)
Saisir son NPI	Citoyen /Résident	Après le lancement de l'application, le citoyen/résident doit saisir son NPI dans le champ correspondant. Si le NPI est correct, le système poursuit les étapes suivantes, sinon le citoyen doit ressaisir son NPI
Vérifier s'il y a un compte déjà actif	Système d'identification	Le système d'identification vérifiera s'il y a un compte déjà actif pour le NPI en question
Compte mobile ID trouvé ?	Système d'identification	Si le système d'identification ne trouve pas un compte actif pour le NPI saisi il pourra suivre avec les étapes suivantes. Si un compte existe déjà, le process prend fin
Compte portail fID trouvé ?	Système d'identification	
Cliquer sur « recevoir OTP »	Citoyen /Résident	Si le citoyen a déjà un compte, il clique sur le bouton « Recevoir OTP », en choisissant le canal de réception de l'OTP soit par SMS soit par mail.
Créer et confirmer un mot de passe	Citoyen /Résident	Le citoyen/résident doit créer et confirmer un mot de passe. Le mot de passe doit respecter les règles suivantes : • Une taille minimale de 10 caractères. • Contient au moins une lettre en majuscule • Contient au moins une lettre en minuscule • Contient au moins un chiffre. • Contient au moins un caractère spécial (#, @, *, etc.)
Consentir sur la politique de gestion des données personnelles	Citoyen /Résident	Le citoyen/résident lit et accorde son consentement à la politique de protection des données personnelles. Cette politique doit indiquer clairement les modalités d'utilisation et de partage des données des citoyens en interne et avec les fournisseurs de services.
Générer une question aléatoire de la liste des questions	Système d'identification	Le système d'identification génère une question aléatoire dont la réponse est une information enregistrée dans le système d'identification (exemple : date de naissance du père, date de naissance de la mère, Commune de naissance, Numéro de carte LEPI, etc.)
Répondre à la question posée	Citoyen /Résident	Le citoyen/résident répond à la question posée.
Vérifier la réponse soumise par rapport la réponse stockée.	Système d'identification	Le système d'identification traite la réponse soumise par le citoyen/résident et fait une vérification par rapport la réponse stockée lors de l'enregistrement.
Activer le compte sur le portail fID	ANIP / centre de vérification	Une fois que les conditions de vérification sont satisfaites, le compte portail fID du citoyen/résident est activé.

Tableau 14 : Description des étapes du processus création d'un compte portail fID

3.5 Login portail fID

Une fois le compte sur le portail créé, le citoyen/résident aura l'opportunité d'accéder aux différents services, et tout comme pour l'application mobile, il doit s'authentifier pour accéder à son compte : c'est le processus login portail fID, détaillé dans le graphique suivant.

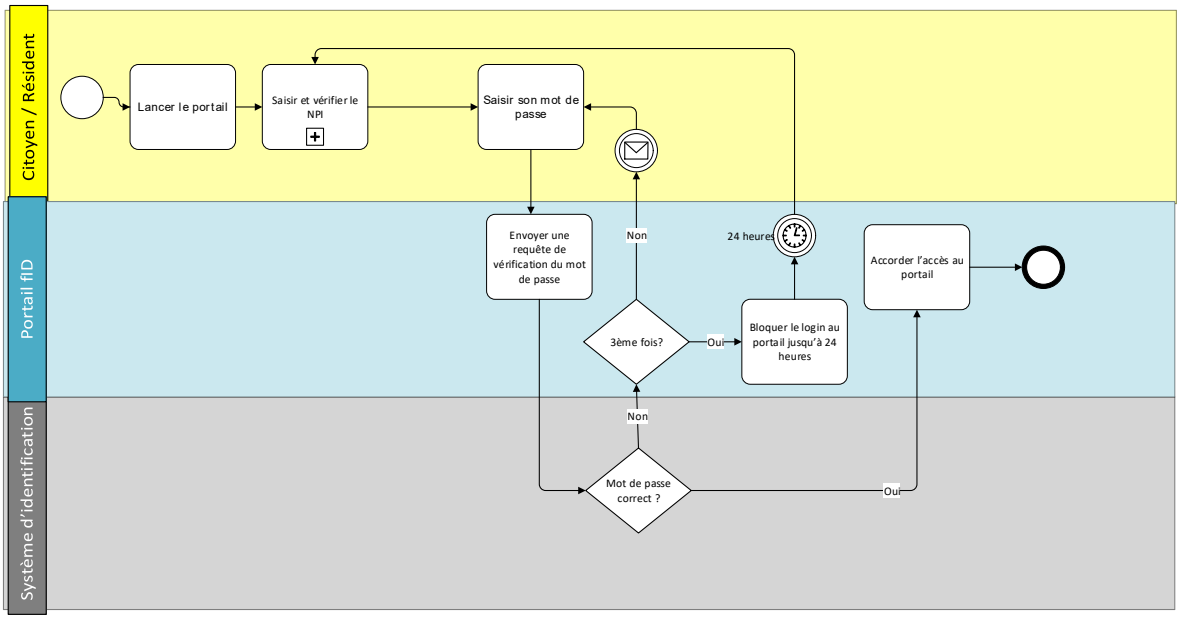


Figure 15 : Processus de login au portail fID

Ci-dessous le tableau descriptif de l'ensemble des étapes du processus.

Etape	Responsable/Système	Description
Lancer le portail	Citoyen / résident	Le citoyen/résident lance le portail en utilisant un navigateur web.
Saisir son NPI	Citoyen / résident	Le citoyen/résident saisit son NPI et clique sur le bouton « Suivant ».
Envoyer une requête de vérification du NPI.	Portail fID	Le portail fID envoi une requête de vérification du NPI au moteur de déduplication du système d'identification.
NPI existant ?	Système d'identification	Le système d'identification répondra s'il a trouvé le NPI saisi ou pas. Si le NPI est introuvable, le citoyen/résident sera amené de nouveau à la page de saisi du NPI, sinon l'étape suivante sera déclenchée.
Saisir son mot de passe.	Citoyen / résident	Le citoyen/résident saisit le mot de passe qu'il a défini dans le processus de création de compte portail fID.
Envoyer une requête de vérification du mot de passe	Portail fID	Le portail fID envoie une requête de vérification du mot de passe au système d'identification.
Mot de passe correct ?	Système d'identification	Le système d'identification vérifie l'authenticité du mot de passe saisi par le citoyen/résident. Si le mot

Etape	Responsable/Système	Description
		de passe saisi est authentique, l'étape « Accorder l'accès à l'application » sera déclenché.
3ème fois ?	Portail fID	Le portail fID vérifiera si c'est la troisième fois que le mot de passe entré est incorrect, auquel cas, l'accès à l'application sera bloqué pendant 24 heures et un mail + message envoyé au citoyen/résident enregistré. Sinon le citoyen/résident peut re-saisir son mot de passe.
Accorder l'accès au portail	Portail fID	Après la satisfaction des conditions du login, le citoyen aura l'accès au portail fID et pourra bénéficier des services disponibles.

Tableau 15 : Tableau descriptif du processus de login au portail fID

4 Processus de création des identifiants

4. Création des identifiants

À partir de l'identité unique que possède le citoyen qui est le NPI, trois identifiants distincts peuvent découler pour permettre au citoyen de s'authentifier, à savoir :

- **La carte fID:** Le premier identifiant qui peut découler de cet identifiant unique est la carte fID, cette carte présente un document physique qui contient des informations d'identification du citoyen, telles que son nom, sa date de naissance, ainsi que le NPI.
- **Le Mobile ID:** Le deuxième identifiant créée à partir de l'identifiant unique est le "Mobile ID". Il s'agit d'une d'identité électronique qui est stockée et accessible via un appareil mobile, tel qu'un smartphone. Le Mobile ID peut être utilisé pour des transactions en ligne, la connexion à des services numériques, ou d'autres opérations qui requièrent une authentification mobile.
- **L'IDV:** Le troisième identifiant est l'IDV qui est un numéro aléatoire temporaire et révocable associé au numéro NPI. L'IDV peut être utilisé à la place du numéro NPI chaque fois que des services d'authentification ou d'e-KYC sont effectués. L'authentification peut être effectuée en utilisant L'IDV de manière similaire à l'utilisation du NPI.

Les détails spécifiques sur la création de chaque identité seront expliqués dans cette section

4.1 Délivrance des cartes NPI/fID

Après l'enregistrement du citoyen, une étape suivante consiste à se rendre à l'ANIP et à présenter le récépissé RAVIP en tant que preuve de son enregistrement. À ce stade, l'ANIP formalise la demande reçue et procède à la pré-identification, qui consiste à inclure le citoyen dans la liste des bénéficiaires cibles des cartes fID. La préparation de cette liste des bénéficiaires débute environ deux mois avant le lancement effectif de l'impression des cartes.

Une fois que la liste est finalisée, l'ANIP entame la production des cartes fID, comprenant l'impression des certificats, leur plastification et leur découpe, en tenant compte des normes de qualité technique requises par la Banque mondiale en matière d'attributs du justificatif d'identité. L'objectif est d'assurer une qualité optimale tout en maîtrisant les coûts. L'ANIP s'engage à garantir la qualité dès la première tentative, en suivant le principe de "Faire bien et bon du premier coup".

Ensuite, l'ANIP procède à la distribution des certificats physiques du NPI/fID vers les centres d'enregistrement concernés. L'opérateur d'enregistrement est chargé de contacter le citoyen par e-mail et SMS pour l'informer qu'il doit récupérer sa carte en personne. L'opérateur vérifie l'identité du citoyen en question en utilisant son NPI en conjonction avec un OTP (One-Time Password) ou des données biométriques.

Ci-dessous la figure qui décrit le processus de délivrance des cartes fID

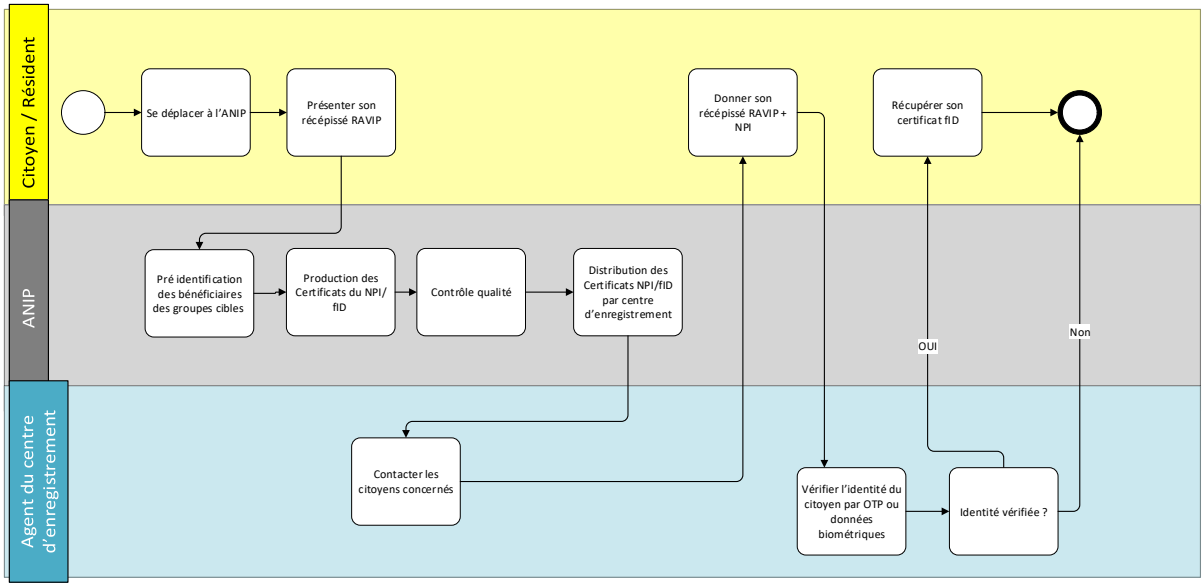


Figure 16 : Processus de délivrance des cartes NPI/fID

Ci-dessous un tableau qui récapitule les étapes de délivrance des cartes NPI/fID.

Etape	Responsable/Système	Description
Se déplacer à l'ANIP	Citoyen / Résident	Le citoyen doit se déplacer physiquement à l'ANIP.
Présenter son récépissé RAVIP	Citoyen / Résident	Le citoyen doit présenter son récépissé RAVIP à l'ANIP comme preuve d'enregistrement
Pré identification des bénéficiaires des groupes cibles	ANIP	L'ANIP pré-identifie les bénéficiaires des cartes fID en les incorporant dans une liste
Production des Certificats du NPI/fID	ANIP	L'ANIP produit les certificats NPI
Contrôle qualité	ANIP	L'ANIP s'engage à garantir une qualité optimale dès la première tentative
Distribution des Certificats NPI/fID par centre d'enregistrement	ANIP	Les certificats sont distribués par l'ANIP aux centres d'enregistrement concernés
Contacter les citoyens concernés	Agent du centre d'enregistrement	L'agent d'enregistrement contacte les citoyens concernés par e-mail et/ou SMS pour les informer qu'ils doivent récupérer leur carte en personne
Donner son récépissé RAVIP + NPI	Citoyen / Résident	Le citoyen doit présenter son récépissé RAVIP et son NPI pour récupérer sa carte
Vérifier l'identité du citoyen par OTP ou données biométriques	Agent du centre d'enregistrement	L'agent d'enregistrement vérifie l'identité du citoyen en utilisant l'OTP ou les données biométriques
Identité vérifiée ?	Agent du centre d'enregistrement	S'assurer de l'identité du citoyen avant de lui remettre sa carte
Récupérer son certificat fID	Agent du centre d'enregistrement	Le citoyen récupère enfin sa carte physique fID

Tableau 16 : Tableau descriptif du processus de délivrance des carte NPI/fID

4.2 Génération d'un IDV

Un IDV (identifiant virtuel) est un numéro aléatoire temporaire et révocable composé de 12 chiffres et associé au numéro NPI. L'IDV peut être utilisé à la place du numéro NPI chaque fois que des services d'authentification ou d'e-KYC sont effectués. Il peut être utilisé au lieu du NPI (notamment pour s'authentifier aux services) pour des raisons de sécurité et de protection des données personnelles. L'IDV permet ainsi au citoyen/résident d'accéder à des services à travers un identifiant temporaire (durée à déterminer) lorsque le citoyen/résident ne souhaite pas partager sont NPI (qui est unique et définitif) pour plusieurs raisons telles que :

- La sécurité : Dans le cas où un service en ligne serait compromis, l'utilisation d'un IDV réduirait le risque associé à l'exposition d'identifiants uniques et permanents.
- La réduction des risques d'usurpation d'identité : Étant donné que l'IDV est temporaire et différent du NPI, cela réduit les chances qu'une personne mal intentionnée puisse usurper l'identité d'une autre personne.
- La protection des données personnelles : L'utilisation d'un IDV permet à un individu d'accéder à des services sans avoir à partager des informations personnelles définitives ou sensibles, comme le NPI.
- Etc,

Ci-dessous le processus pour créer un IDV unique via l'application mobile ou via le portail fID.

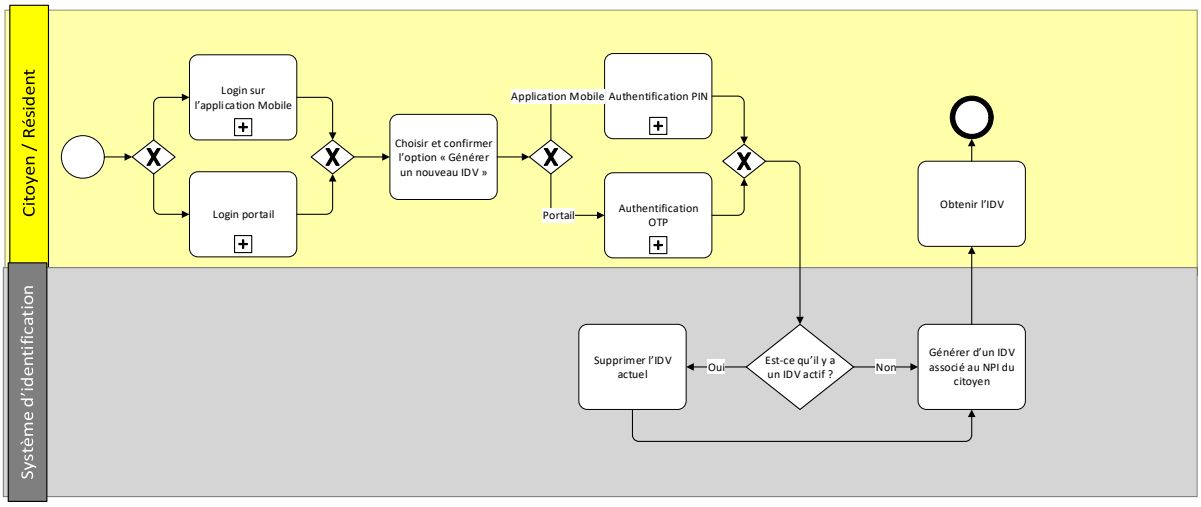


Figure 17 : Processus de génération d'un ID virtuel (IDV)

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus d'obtention d'un IDV.

Etape	Responsable/Système	Description
Login sur l'application mobile	Citoyen / résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login portail fID	Citoyen / résident	

Etape	Responsable/Système	Description
Choisir et confirmer l'option « Générer un nouveau IDV »	Citoyen / résident	Le citoyen/résident accède à l'espace des services. Il doit choisir et confirmer l'option « Générer un nouveau IDV ». Dans le cas où le citoyen/résident a déjà un IDV qui est actif, le message suivant sera affiché « Selon la politique de l'RNPP il n'est possible de garder qu'un seul IDV, si vous procédez à la génération d'un nouveau IDV, l'IDV en cours sera supprimé »
Authentification PIN	Citoyen / résident	Dans le cas où le citoyen/résident utilise l'application mobile, il doit s'authentifier une autre fois en utilisant son PIN
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID, il doit s'authentifier une autre fois en utilisant un OTP qui sera envoyé à son numéro de téléphone déjà enregistré dans la base de données RNPP.
Supprimer l'IDV actuel	Système d'identification	Dans le cas où au moment de la confirmation de l'obtention d'un nouveau IDV, il y a déjà un IDV actif il sera supprimé.
Générer un IDV	Système d'identification	Le système d'identification génère un IDV Différent de tous les IDV créés
Obtenir l'IDV	Citoyen / résident	Le citoyen/résident obtient son IDV sous la forme d'un numéro qu'il peut l'utiliser pour obtenir des services

Tableau 17 : Tableau descriptif du processus d'obtention d'un IDV

4.3 Création et activation du Mobile ID

Le citoyen, après avoir créé son compte dans la section 3.2, accède à l'application mobile et sélectionne l'option pour demander un mobile ID. Ensuite, il accepte les conditions générales et le traitement des données personnelles.

En suivant ces étapes, le citoyen saisit son NPI et capture un selfie à l'aide de son appareil mobile. Cette photo sera comparée avec celle stockée dans la base de données RNPP. Le Mobile ID est activé une fois que l'identité du citoyen est vérifiée avec succès.

Ci-dessous la figure décriant les étapes à suivre pour créer et activer le mobile ID

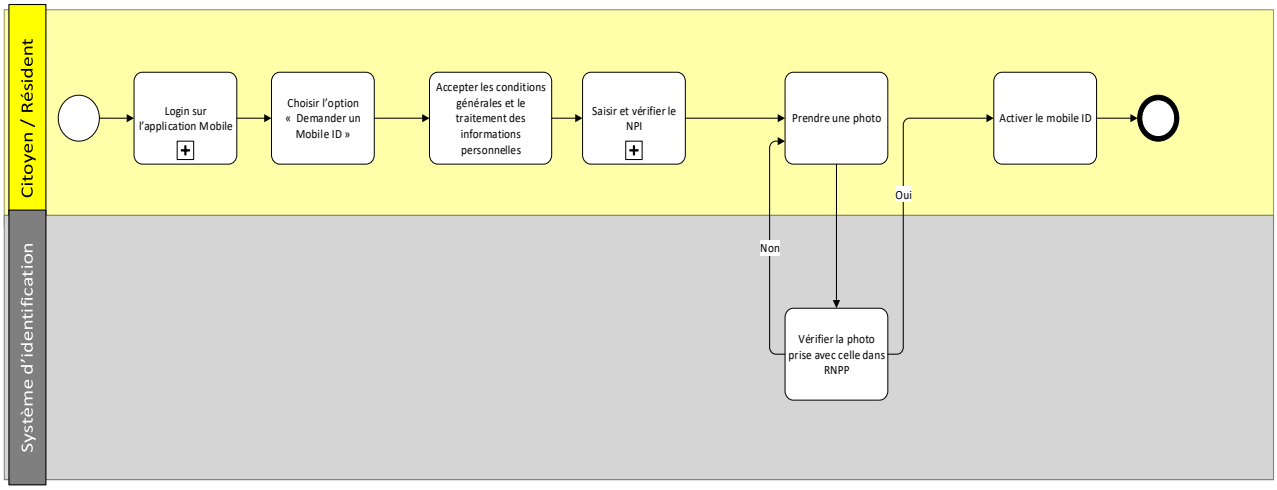


Figure 18 : Processus de création et activation du mobile ID

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de création et activation du mobile ID.

Etape	Responsable/Système	Description
Login sur l'application Mobile	Citoyen / Résident	Le citoyen/résident se connecte à son compte via l'application mobile
Choisir l'option « Demander un Mobile ID »	Citoyen / Résident	Le citoyen/résident sélectionne l'option « Demander un Mobile ID »
Accepter les conditions générales et le traitement des informations personnelles	Citoyen / Résident	Le citoyen accepte obligatoirement les conditions générales et le traitement des informations personnelles
Saisir et vérifier le NPI	Citoyen / Résident	Sous processus « Saisir et vérifier le NPI »
Prendre une photo	Citoyen / Résident	Le citoyen/résident suit les instructions pour prendre une photo de son visage de plusieurs côtés : vue de face, vue de gauche, vue de droite.
Vérifier la photo prise avec celle dans RNPP	Système d'identification	Le système d'identification vérifie la photo prise avec celle dans la base nationale RNPP
Activer le mobile ID	Citoyen / Résident	Si la vérification de la photo est réussite, le mobile ID sera activé

Tableau 18 : Tableau descriptif du processus de création et activation du mobile ID

5 Processus d'authentification en ligne

5. Processus d'authentification en ligne

Dans cette section, nous examinerons de près les modalités d'authentification en ligne en fonction des situations qui requièrent cette authentification. Nous serons dans le cas de figure où le citoyen/résident utilise un terminal connecté à Internet, tel qu'un smartphone, un ordinateur, une tablette, etc., pour :

- Se connecter à un compte application mobile ;
- Se connecter à un compte portail fID ;
- Accéder à des services : pour accéder aux services, le fournisseur de service définit les modalités d'authentification (nombre de facteurs d'authentification par service) et à chaque demande de service, un mail et un SMS sont envoyés à l'utilisateur pour l'informer de l'action d'authentification, l'authentification à un service d'un fournisseur de service n'induit pas automatiquement une authentification aux services d'un autre fournisseur

Il faut noter que lorsque le citoyen n'est pas actif pendant 5 min ou se déconnecte il est dans l'obligation de se connecter à nouveau et de s'authentifier à nouveau pour accéder à un service d'un fournisseur.

Le citoyen ou le résident pourra s'authentifier en ligne via plusieurs méthodes :

- Si le citoyen/résident accède via l'application mobile : Dans ce cas, 2 facteurs d'authentification sont possibles à savoir le mot de passe ou le code PIN (le PIN est initié à la création du compte mobile, communément utilisé pour simplifier l'authentification mobile et la rendre plus rapide).
- Si le citoyen/résident accède via le portail fID : Dans ce cas, 2 facteurs d'authentification sont possibles à savoir le mot de passe, ou le code OTP (l'OTP est temporaire et communément utilisé pour valider une opération ou l'accès à un service via le portail web).

5.1 Authentification en ligne par OTP

Un OTP est un code qui n'est valable qu'une seule fois pour une session d'authentification ou une transaction spécifique. Une fois utilisé, il ne peut plus être réutilisé.

L'option d'authentification en ligne via OTP pourra être disponible pour vérifier l'identité des utilisateurs lorsqu'ils souhaitent accéder à un service sur le portail fID (pour le mobile ID, différentes méthodes d'authentification ont été envisagées et seront abordées ultérieurement).

Comme le montre la figure suivante, le processus d'authentification en ligne pour accéder à un service sur le portail fID commence lorsque le citoyen/résident cherche à bénéficier d'un service bien défini.

La figure ci-dessous illustre le processus d'authentification en ligne par OTP sur le portail fID, détaillant chaque étape depuis la demande initiale jusqu'à la fourniture du service demandé.

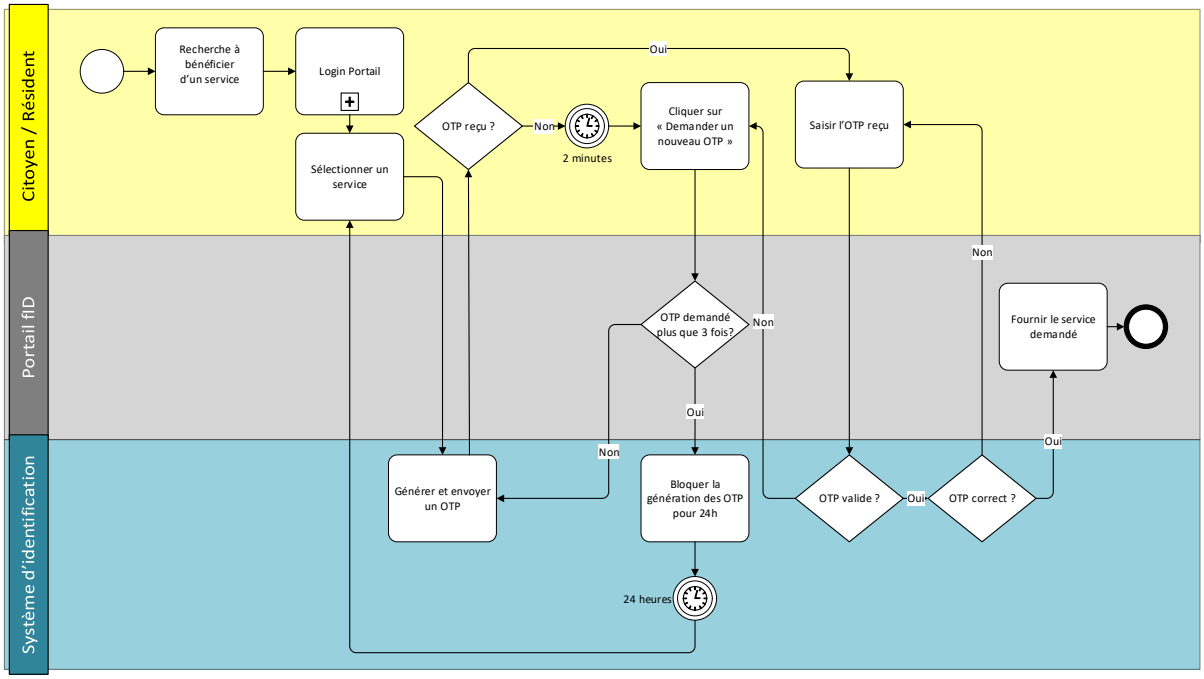


Figure 19 : Processus d'authentification OTP en ligne

Le citoyen/résident s'étant préalablement connecté au portail fID, et ayant accédé à la rubrique des services disponibles, recevra un code OTP généré par le système et envoyé au numéro de téléphone associé au NPI du citoyen dans la base de données RNPP.

Le citoyen/résident vérifiera la réception de l'OTP dans un délai de 2 minutes, au-delà duquel il pourra en demander un nouveau. Une fois l'OTP reçu, le citoyen/résident peut le saisir dans l'interface.

Le système d'identification vérifie d'abord la validité de l'OTP, si l'OTP n'est plus valide, le citoyen doit en demander un nouveau avec une limite de trois OTP par jour pour un même service, en cas de quatrième demande d'OTP pour ce même service en une journée, le système d'identification bloquera la génération des OTP pendant 24 heures.

Ensuite, le système vérifie si l'OTP saisi par le citoyen/résident est correct. Si le citoyen/résident ne saisit pas correctement l'OTP, le citoyen/résident peut réessayer autant de fois que nécessaire tant que l'OTP reste valide. Lorsque l'OTP est correct, le portail fID fournira alors le service demandé.

Ce processus assure à la fois la sécurité et la gestion appropriée des demandes d'OTP pour l'accès aux services sur le portail fID.

Ci-dessous un tableau qui récapitule les étapes décrites plus haut.

Etape	Responsable/Système	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident cherche à bénéficier d'un service disponible sur le portail fID.
Login portail	Citoyen / résident	Le citoyen/résident suit les étapes du processus de login au portail fID.

Etape	Responsable/Système	Description
Sélectionner un service	Citoyen / résident	Le citoyen/résident demande le service dont il a besoin dans la rubrique des services disponibles.
Générer et envoyer un OTP	Système d'identification	Le système génère et envoie un OTP au numéro de téléphone correspondant au NPI du citoyen enregistré dans la base de données RNPP.
OTP reçu ?	Citoyen / résident	Le citoyen/résident vérifiera s'il a reçu le code OTP. Après 2 minutes, le citoyen peut demander un nouvel OTP.
Saisir l'OTP reçu	Citoyen / résident	Le citoyen/résident saisit l'OTP reçu sur son téléphone
OTP valide ?	Système d'identification	Le système d'identification vérifie en premier lieu si l'OTP est encore valide. La durée de validité de l'OTP est 2 minutes à compter à partir du moment de l'envoi. Dans le cas où l'OTP n'est plus valide, le citoyen doit demander un nouvel OTP.
OTP correct ?	Système d'identification	Le système vérifie si l'OTP saisi par le citoyen/résident est correct. Dans le cas où l'OTP saisi n'est pas correct, le citoyen peut tenter sans limite tant que l'OTP est encore valide.
Fournir le service demandé	Portail fID	Dans le cas où l'OTP est correct, le portail fID procédera à la fourniture du service demandé.
Cliquer sur « Demander un nouvel OTP »	Citoyen / résident	Dans le cas où l'OTP envoyé n'est plus valide, le citoyen/résident peut demander un autre OTP avec un plafond de trois OTP par jour par service.
OTP demandé plus que 3 fois ?	Portail fID	Le système vérifiera si le citoyen a demandé un OTP plus que trois fois par jour pour le même service.
Bloquer la génération des OTP pendant 24h	Système d'identification	A la quatrième demande d'OTP par jour pour le même service, le système d'identification bloquera la génération des OTPs pour 24 heures

Tableau 19 : Tableau descriptif du processus d'authentification OTP en ligne

5.2 Authentification par PIN

Un code PIN est un numéro confidentiel composé de chiffres, souvent quatre, six ou huit chiffres, utilisé généralement pour authentifier une personne voulante accéder à des systèmes informatiques sécurisés.

La forme et la structure du code PIN est différente de celle du mot de passe, qui lui est généralement constitué d'une combinaison de lettres, de chiffres et de caractères spéciaux. En effet le code PIN est un code permanent qui est souvent plus court et est généralement utilisé pour des accès rapides et fréquents.

L'option d'authentification en ligne par PIN, illustrée par le schéma suivant, est utilisée pour accéder à l'application mobile une fois que la vérification du NPI a été effectuée et que l'option authentification par PIN est choisie. Elle est également utilisée pour confirmer une demande de service d'identité sur l'application mobile.

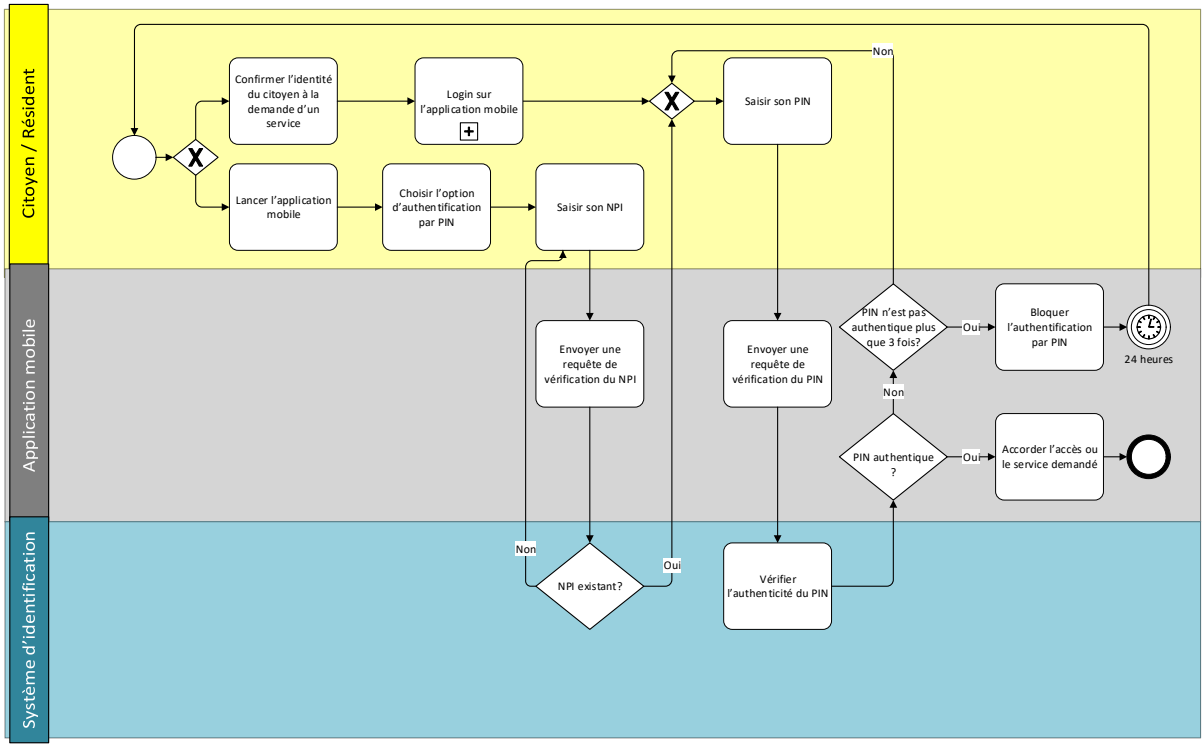


Figure 20 : Processus d'authentification par PIN d'authentification

Pour se connecter à l'application mobile, le citoyen/résident doit d'abord saisir son NPI. L'application envoie alors une requête au système d'identification pour vérifier la validité du NPI saisi. Si le NPI est introuvable, le citoyen/résident est invité à entrer un NPI valide pour poursuivre. Une fois qu'un NPI valide est saisi le citoyen/résident a le choix de s'authentifier par code PIN ou par mot de passe.

Lors du déclenchement de l'authentification par PIN, qu'elle soit pour une connexion à l'application mobile ou pour une demande d'un nouveau service, le citoyen/résident doit entrer le PIN qu'il a défini lors de la création de son compte. L'application envoie alors une requête au système d'identification pour vérifier le PIN saisi, utilisant le PKI national pour garantir l'authenticité.

Le système d'identification surveille le nombre de tentatives d'authentification et vérifie si le citoyen/résident a atteint le seuil fixé (généralement trois tentatives pour une opération d'authentification). Si le citoyen/résident saisit un PIN non authentique trois fois de suite, l'authentification par PIN sera bloquée à la quatrième tentative pour une période de 24 heures et un message sera envoyé au citoyen/résident concerné par mail et par SMS pour lui notifier de l'action de blocage de l'authentification par PIN.

En revanche, si le PIN est authentique, le citoyen/résident obtient l'accès à l'application ou au service demandé, garantissant ainsi un niveau de sécurité optimisé tout en facilitant l'utilisation de l'application mobile.

Ci-dessous un tableau qui récapitule les étapes décrites plus haut et liées au processus d'authentification par PIN.

Etape	Responsable/Système	Description
Lancer l'application mobile	Citoyen / résident	L'authentification par PIN est proposée à la fois pour accéder à l'application mobile après la vérification du NPI et pour la confirmation d'une demande d'un service d'identité.
Confirmer la demande d'un service d'identité sur l'application mobile	Citoyen / résident	
Saisir son NPI	Citoyen / résident	Afin d'accéder à l'application, le citoyen/résident doit saisir en premier lieu son NPI.
Envoyer une requête de vérification du NPI	Application mobile	L'application mobile envoie une requête au système d'identification pour vérifier le NPI saisi
NPI existant ?	Système d'identification	Le système d'identification répond à la requête envoyée. Dans le cas où le NPI est introuvable, le citoyen/résident doit saisir un NPI valide pour passer à l'étape suivante.
Saisir son PIN	Citoyen / résident	Après la saisie d'un NPI valide ou la confirmation de la demande d'un service, le citoyen/résident doit saisir le PIN qu'il a défini lors de la création de son compte.
Envoyer une requête de vérification du PIN	Application mobile	L'application mobile envoie une requête au système d'identification pour vérifier le PIN saisi.
Vérifier l'authenticité du PIN	Système d'identification	Le système d'identification vérifiera l'authenticité du PIN à l'aide du PKI national.
Vérifier si le code PIN a été entré de manière incorrecte pour plus que trois fois	Application mobile	Le système vérifie à chaque tentative si le citoyen/résident a atteint le seuil de tentatives fixé ou pas (trois tentatives pour une opération d'authentification).
Bloquer l'authentification par PIN	Application mobile	Dans le cas où le citoyen/résident a saisi un PIN non authentique 3 fois, l'authentification par PIN sera bloquée à la quatrième tentative pendant 24 heures.
Envoyer un message par mail et SMS	Système d'identification	Un message sera envoyé par mail et SMS pour notifier le citoyen/résident qu'il sera inaccessible pour les trois prochaines heures.
Accorder l'accès ou le service demandé	Application mobile	Dans le cas où le PIN est authentique, le citoyen/résident aura l'accès à l'application ou au service demandé

Tableau 20 : Tableau descriptif du processus d'authentification par PIN

5.3 Authentification par mot de passe

L'option de l'authentification en ligne par mot de passe est possible lors de connexion au compte portail fID ou mobile ID.

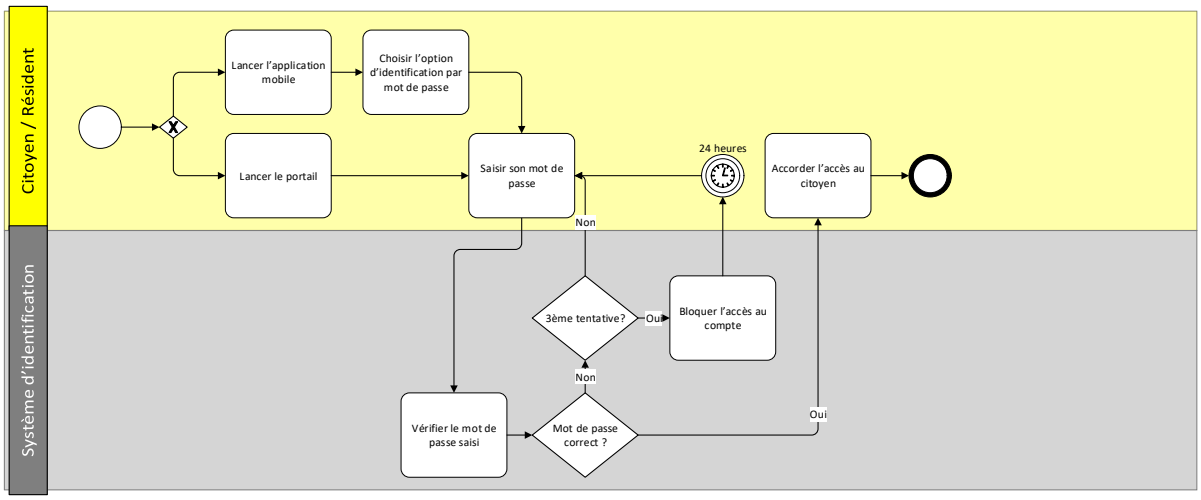


Figure 21 : Processus d'authentification par mot de passe

Le processus d'authentification par mot de passe est possible lors de la connexion au compte portail fID ou son application mobile. Le citoyen/résident commence par lancer l'application sur son téléphone ou par accéder au portail fID via un navigateur web.

Dans le cas d'une connexion à travers l'application mobile, le citoyen/résident a le choix de s'authentifier par mot de passe ou par PIN. Si l'option d'authentification par mot de passe est choisie, Ie citoyen saisit le mot de passe qu'il a préalablement entré lors de la création du compte.

Le système d'identification vérifie le mot de passe saisi en le comparant à celui enregistré dans la base de données. Si le citoyen/résident entre un mot de passe incorrect trois fois de suite, l'accès à son compte sera temporairement bloqué, pour une période de 24 heures.

Cependant, si le mot de passe saisi est correct, l'accès au portail ou à l'application mobile sera accordé, permettant ainsi à l'utilisateur d'utiliser les services associés en toute sécurité.

Ci-dessous un tableau qui récapitule les étapes décrites plus haut, en lien avec le processus d'authentification par mot de passe.

Etape	Responsable/Système	Description
Lancer l'application	Citoyen / résident	L'authentification par mot de passe est possible lors de connexion au compte portail fID ou à l'application mobile. Le citoyen/résident commence par lancer l'application sur son téléphone ou le portail fID à l'aide du navigateur internet.
Lancer le portail	Citoyen / résident	
Choisir de s'authentifier par mot de passe.	Citoyen / résident	Pour l'application mobile, il est possible de choisir de s'authentifier par mot de passe ou par PIN.
Saisir son mot de passe.	Citoyen / résident	Le citoyen/résident saisit le mot de passe qu'il a entré lors de l'opération de création du compte.
Vérifier le mot de passe saisi.	Système d'identification	Le système d'identification vérifie le mot de passe saisi par rapport au mot de passe enregistré dans la base de données.

Etape	Responsable/Système	Description
Bloquer l'accès au compte	Système d'identification	Dans le cas où le citoyen/résident a saisi un mot de passe incorrect trois fois, l'accès à son compte sera bloqué pendant 24 heures.
Accorder l'accès au citoyen	Système d'identification	Dans le cas où le mot de passe saisi par le citoyen/résident est correct, l'accès au portail ou à l'application mobile sera accordé.

Tableau 21 : Tableau descriptif du processus d'authentification par mot de passe

5.4 Authentification en ligne à 2 facteurs

L'authentification à 2 facteurs est une authentification qui permet de renforcer la sécurité des accès. La particularité de ce mode d'authentification est de demander à l'utilisateur plusieurs éléments de preuves, qu'on appelle facteurs, afin de confirmer son identité.

Dans le cas d'une authentification en ligne, il est techniquement possible de combiner plusieurs facteurs tels que mot de passe, code PIN et code OTP et ces modalités d'authentification sont définies par le fournisseur de service (nombre de facteurs d'authentification par service) en fonction de la sensibilité de son service sachant que le système d'identification fournira tous les éléments techniques nécessaires à cette authentification.

Comme le montre la figure suivante, nous avons fait le choix de distinguer l'authentification en ligne à 2 facteurs soit à travers la connexion via l'application mobile ou à travers la connexion via le portail.

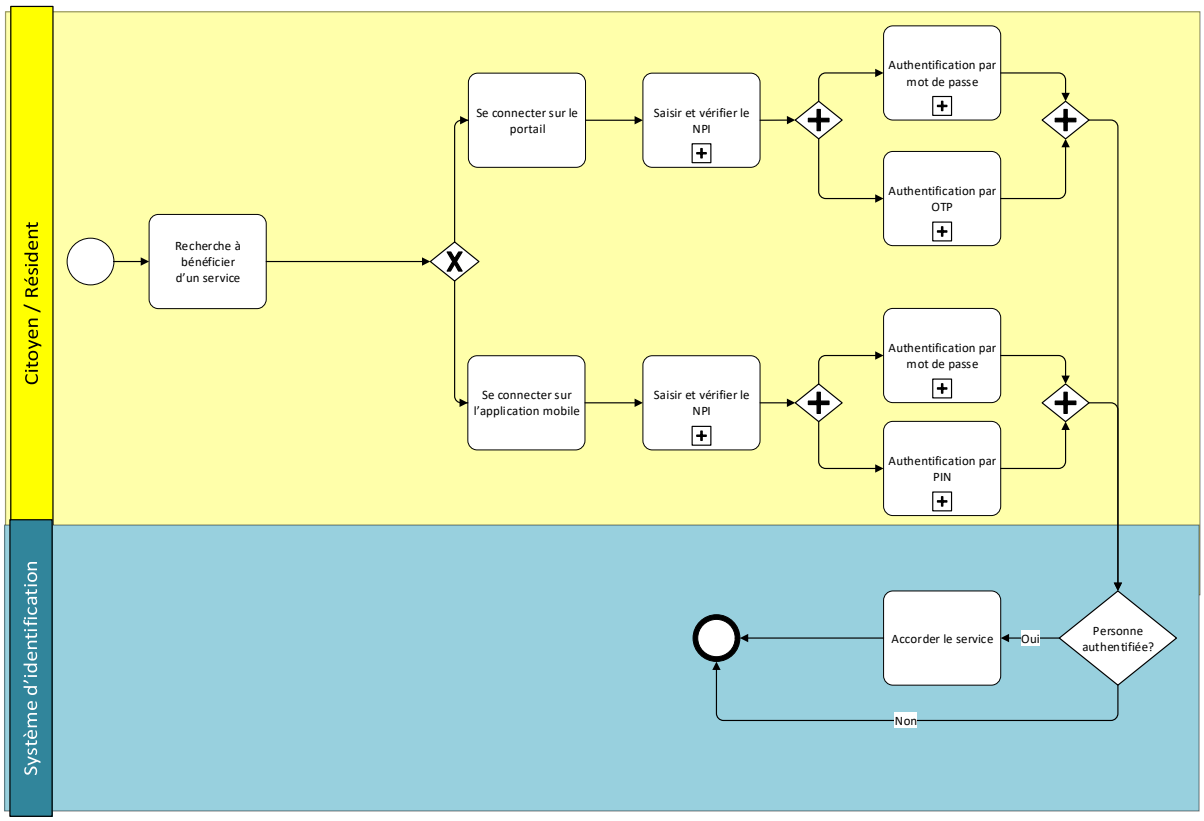


Figure 22 : Processus d'authentification en ligne à 2 facteurs

Le tableau suivant explique les principales étapes de ce processus.

Etape	Responsable	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident cherche à bénéficier d'un service chez un fournisseur de service public ou privé.
Option 1 : connexion via le portail	Citoyen / résident	Le citoyen/résident se connecte au portail fID
Saisir et vérifier son NPI	Citoyen / résident	Le citoyen/résident fournit son NPI au fournisseur de service pour s'authentifier.
Saisir les informations d'authentification demandées	Citoyen / résident	Le citoyen/résident saisit les informations demandées : • Mot de passe • OTP
Option 2 : connexion via l'application mobile	Citoyen / résident	Le citoyen/résident se connecte à l'application mobile

Etape	Responsable	Description
Saisir et vérifier son NPI	Citoyen / résident	Le citoyen/résident fournit son NPI au fournisseur de service pour s'authentifier.
Saisir les informations d'authentification demandées	Citoyen / résident	Le citoyen/résident saisit les informations demandées : • Mot de passe • PIN

Tableau 22 : Tableau descriptif du processus d'authentification en ligne à 2 facteurs

6 Processus d'authentification hors ligne

6. Processus d'authentification hors ligne

Le processus d'authentification :

- Citoyen hors ligne se réfère à un déplacement physique du citoyen/résident chez le fournisseur de service pour confirmer son identité, dans ce cas, les modalités d'authentification suivantes sont possibles : authentification par carte fID authentification biométrique, authentification e-kYC et authentification par mobile ID.
- Fournisseur de service hors ligne implique que, outre le fait que le citoyen soit physiquement présent lors de la procédure, le fournisseur de service n'a pas accès à une connexion Internet. Malgré l'absence de connectivité en ligne, le fournisseur de service doit néanmoins être en mesure d'authentifier le citoyen.

6.1 Citoyen hors ligne : Authentification biométrique

L'authentification biométrique est un processus de vérification de l'identité d'une personne qui se base sur ses caractéristiques physiologiques ou comportementales uniques et mesurables. Contrairement aux méthodes d'authentification traditionnelles telles que le mot de passe ou le code PIN, l'authentification biométrique repose sur des caractéristiques inhérentes à l'individu, ce qui en fait une méthode particulièrement sécurisée. Les caractéristiques biométriques du client peuvent être le visage ou l'empreinte.

- Pour le visage : Il faut s'assurer que les traits faciaux soient visibles et reconnaissables, et demander à enlever tout objets ou accessoires qui risqueraient de compromettre l'identification de la structure faciale biométrique comme les lunettes, chapeaux et casquettes de tout type, il faut également veiller à ce que la personne garde une position fixe devant la caméra.

- Pour les empreintes il faut choisir le doigt à scanner et bien le nettoyer avant l'opération avant de le poser dans une position neutre.

Ci-après la figure qui décrit l'ensemble des étapes qui composent le processus d'authentification biométrique, ce processus commence quand le citoyen/résident se déplace vers un fournisseur de service, il lui sera alors demandé de scanner la partie du corps concernée que le fournisseur choisit en notant que cette partie du corps doit préalablement faire partir des données biométriques prises et stockées et en

s'assurant que la qualité de la prise est acceptable. Une fois l'authentification effectuée avec succès le service sera accordé au citoyen/résident.

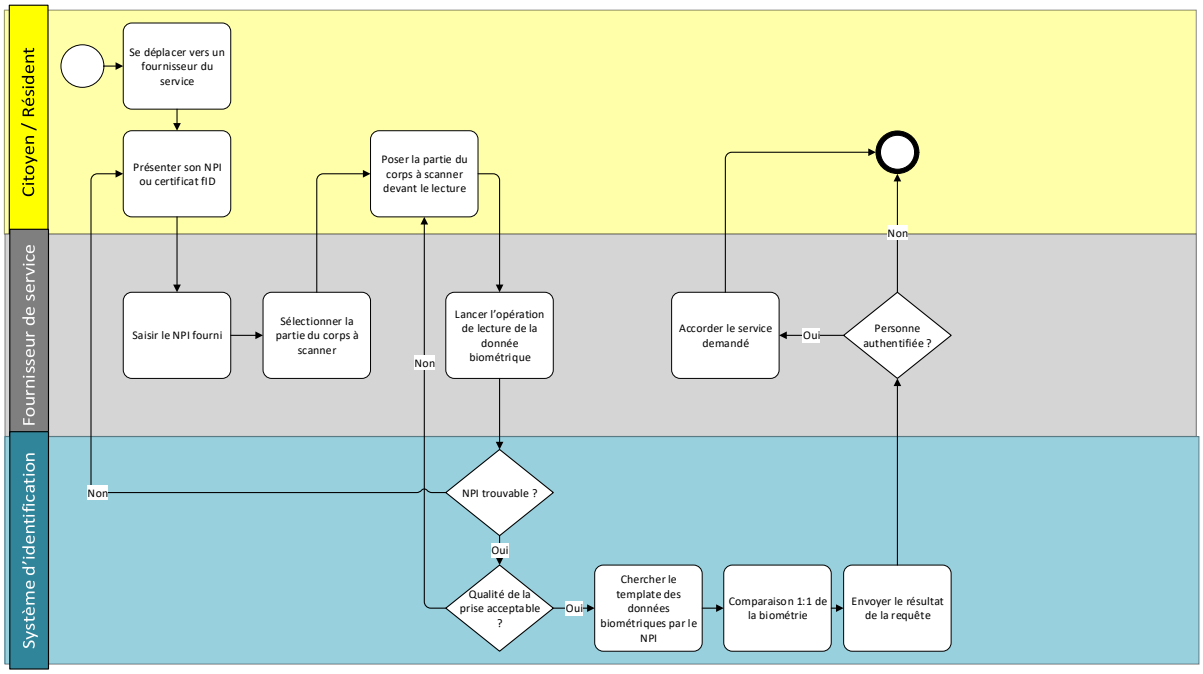


Figure 23 : Processus d'authentification biométrique

Ci-dessous un tableau qui récapitule les étapes décrites plus haut en lien avec le processus d'authentification biométrique

Etape	Responsable	Description
Se déplacer à un fournisseur de service	Citoyen / résident	Le citoyen/résident se déplace physiquement pour bénéficier d'un service.
Présenter son NPI ou son certificat fID	Citoyen / résident	Le citoyen/résident doit présenter son certificat fID ou son NPI au fournisseur de service pour commencer l'opération d'authentification
Saisir le NPI fourni	Fournisseur de service	Le fournisseur de service saisit le NPI fourni par le citoyen/résident dans l'interface d'authentification.
Sélectionner la partie du corps à scanner	Fournisseur de service	Le fournisseur de service sélectionne la donnée biométrique à scanner : visage ou empreinte. Dans le cas de l'empreinte, il faut choisir le doit à scanner aussi
Poser la partie du corps à scanner devant le lecteur	Citoyen / résident	Le citoyen/résident suit les instructions du fournisseur de service dans le positionnement de la biométrie avant de lancer l'opération de lecture. Ces instructions peuvent être : Pour le visage : • Enlever les lunettes solaires ou de vue. • Enlever chapeau et casquette. • Garder une position fixe devant la caméra. Pour les empreintes : • Se nettoyer le doigt à scanner.

Etape	Responsable	Description
		• Poser la totalité de la phalange distale du doigt à scanner dans une position neutre (n'est pas inclinée).
Lancer l'opération de lecture de la donnée biométrique	Fournisseur de service	Le fournisseur de service vérifie que le citoyen/résident a bien respecté les instructions et lance l'opération de lecture. Finalement le fournisseur de service lance la requête d'authentification
NPI trouvable ?	Système d'identification	Le système d'identification commence par la vérification du NPI saisi
Qualité de la prise acceptable ?	Système d'identification	Dans le cas où le système a trouvé NPI saisi, il passe à l'analyse de la qualité de la prise biométrique. Dans le cas où la qualité de la prise n'est pas acceptable par le système, le citoyen/résident doit refaire l'opération de prise de la biométrie
Chercher le template des données biométriques par le NPI	Système d'identification	Dans le cas où la qualité de la prise biométrique est acceptable, le système d'identification utilise le NPI et le type de la donnée biométrique (le doigt dans le cas de l'empreinte) pour identifier le template biométrique à utiliser pour l'opération de l'authentification.
Comparaison 1:1 de la biométrie	Système d'identification	Le système d'identification fait une comparaison entre le template stockée dans la base de données et le template issu de l'opération de lecture de la biométrie
Envoyer le résultat de la requête	Système d'identification	Le système d'identification envoie le résultat de la requête d'authentification au fournisseur de service
Accorder le service demandé	Fournisseur de service	Dans le cas où la personne est authentifiée, le fournisseur de service peut accorder le service demandé au citoyen/résident.

Tableau 23 : Tableau descriptif du processus d'authentification biométrique

6.2 Citoyen hors ligne : Authentification e-KYC

Le processus d'authentification e-KYC est généralement indépendant de la modalité d'authentification spécifique utilisée par le fournisseur de service, qu'il s'agisse de l'authentification biométrique, démographique ou d'une autre méthode. Ce processus se concentre principalement sur la vérification des données et des informations partagées avec le fournisseur de service à la suite de l'opération d'authentification. Le type d'informations partagé dépend donc du fournisseur et de l'accord du citoyen/résident pour le partage de ces informations.

L'authentification e-KYC vise à confirmer l'identité du client en se basant sur les informations qu'il fournit lors de son inscription ou de sa demande de service en ligne. Ces informations peuvent inclure des données personnelles telles que le nom, la date de naissance, l'adresse, le numéro d'identification, etc. voire plus.

Cela permet de garantir que les transactions électroniques et les services en ligne sont utilisés par des personnes authentifiés, disposant des droits et de la légitimité nécessaire.

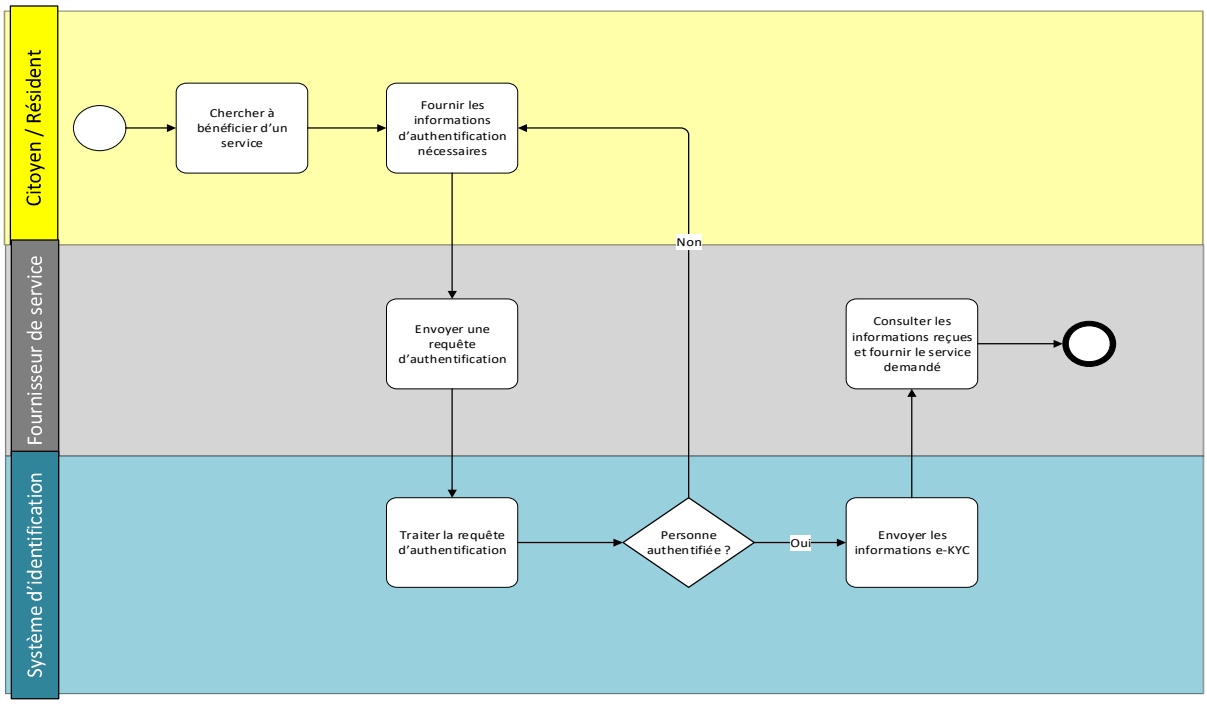


Figure 24 : Processus d'authentification e-KYC

Lorsque le citoyen/résident se rend physiquement chez un fournisseur de service, dans le but de bénéficier d'un service, il doit fournir les informations d'authentification requises en fonction de la méthode d'authentification choisie par le fournisseur de service. Ces informations peuvent prendre différentes formes, telles que les données biométriques, le Numéro Personnel d'Identification (NPI) ou le certificat NPI/fID.

Une fois que le citoyen/résident a fourni ces informations d'authentification, le fournisseur de service envoie une requête au système d'identification pour vérifier que la personne présente est bien celle qu'elle prétend être.

Le système d'identification prend ensuite en charge le traitement de la requête d'authentification en effectuant les vérifications nécessaires en fonction de la méthode d'authentification choisie.

Une fois que le système d'identification a confirmé l'authenticité de la personne, il envoie les informations du citoyen/résident authentifié au fournisseur de service, en conformité avec la politique de traitement des données personnelles en vigueur.

Le fournisseur de service peut alors consulter les informations reçues et fournir les services demandés par le citoyen/résident, garantissant ainsi un processus d'authentification sécurisé et fiable pour l'accès aux services.

Ci-dessous un tableau qui récapitule les étapes décrites plus haut en lien avec le processus d'authentification e-KYC.

Etape	Responsable/Système	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident se déplace physiquement chez un fournisseur de service pour bénéficier d'un service.
Fournir les informations d'authentification nécessaires.	Citoyen / résident	Le citoyen/résident doit fournir les informations d'authentification nécessaires selon la modalité d'authentification utilisée par le fournisseur de service à savoir : • Les données biométriques • Le NPI • Le certificat NPI/fID
Envoyer une requête d'authentification	Fournisseur de service	Le fournisseur de service envoie une requête au système d'identification pour vérifier qu'il s'agit de la bonne personne
Traiter la requête d'authentification	Système d'identification	Le système d'identification prend en charge le traitement de la requête d'authentification faisant les vérifications nécessaires selon la modalité d'authentification utilisée : • Authentification biométrique 1 :1 • Vérification de l'authenticité du QR code • etc
Envoyer les informations e-KYC	Système d'identification	Le système d'identification envoie les informations du citoyen/résident authentifié selon la politique de traitement des données personnelles en vigueur
Consulter les informations reçues et fournir le service demandé	Fournisseur de service	Dans le cas où la personne est authentifiée, le fournisseur de service peut consulter les informations reçues et peut fournir les services demandés

Tableau 24 : Tableau description des étapes du processus authentification e-KYC

6.3 Citoyen hors ligne : Authentification hors ligne à 2 Facteurs :

6.3.1 Authentification par Carte fID + biométrie ou OTP

Le citoyen a la possibilité de se rendre en personne chez un fournisseur de services avec sa carte fID. Tout d'abord, le fournisseur doit scanner le QR code présent sur la carte afin de vérifier son authenticité grâce à l'application de vérification des identités. Une fois que l'authenticité de la carte est confirmée, le fournisseur saisit le Numéro d'Identification Personnel (NPI) qui figure sur la carte (cette étape peut être automatisée). Ensuite, il demande une authentification, qui peut être réalisée soit par un One-Time Password (OTP), soit par une méthode biométrique, telle qu'une vérification du visage ou de l'empreinte, pour valider l'identité du citoyen.

Après avoir authentifié le citoyen avec succès, le fournisseur peut alors procéder à la demande de service du citoyen.

Ci-dessous la figure qui détaille les étapes en cas d'authentification par carte fID et biométrie/PIN

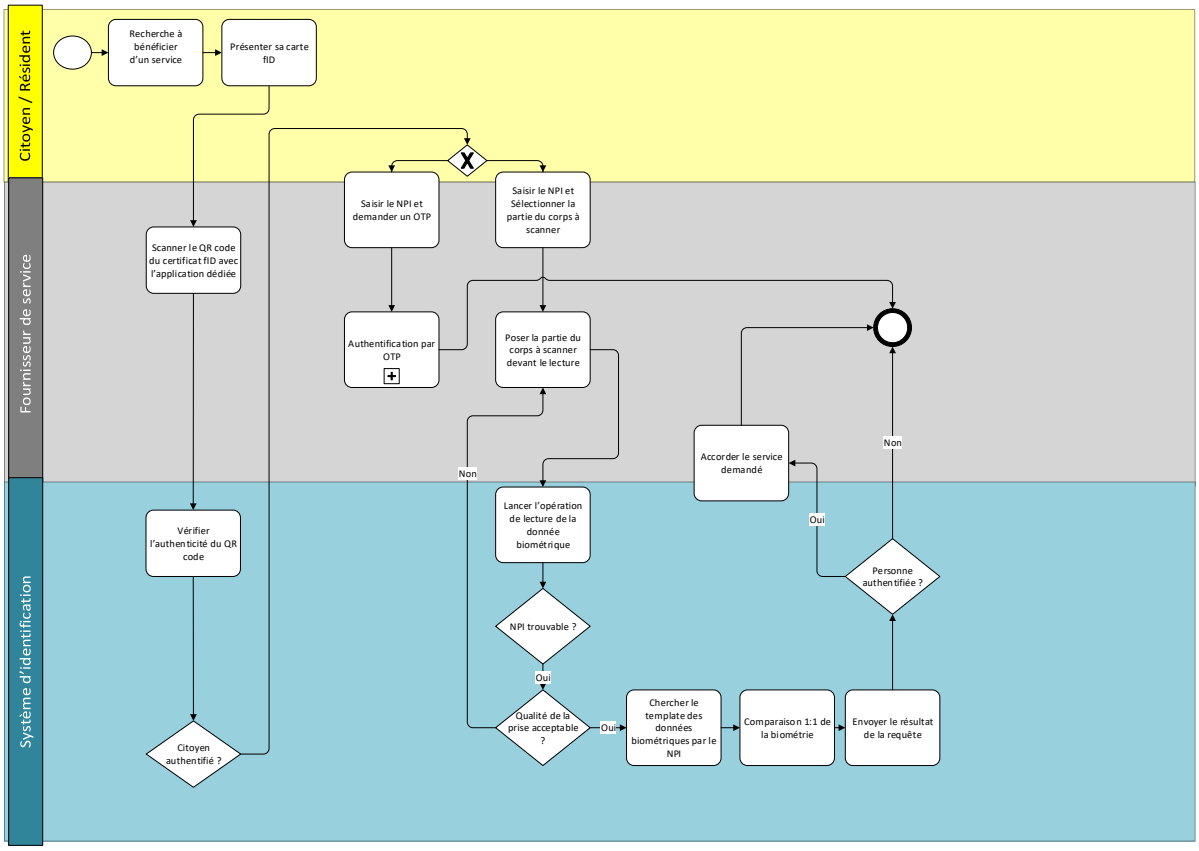


Figure 25 : Processus d'authentification par carte fID

Ci-dessous un tableau qui récapitule les étapes décrites plus haut en lien avec le processus d'authentification par carte fID.

Etape	Responsable/Système	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident se déplace physiquement chez un fournisseur de service pour bénéficier d'un service.
Présenter sa carte fID	Citoyen / résident	Le citoyen se présente physiquement sa carte fID
Scanner le QR code du certificat fID avec l'application dédiée	Fournisseur de service	Le fournisseur utilise une application dédiée pour scanner le QR code présent sur la carte fID.
Vérifier l'authenticité du QR code	Système d'identification	Le système d'identification vérifie l'authenticité du QR code scanné
Citoyen authentifié ?	Système d'identification	Le système d'identification confirme l'authenticité de la carte fID
Option 1 : Saisir le NPI et demander un OTP	Fournisseur de service	Le fournisseur saisit le NPI présent sur la carte fID (cette étape peut être automatisée) et demande une authentification par OTP

Etape	Responsable/Système	Description
Authentification par OTP	Fournisseur de service	Sous processus « Authentification par OTP »
Option2 : Saisir le NPI et Sélectionner la partie du corps à scanner	Fournisseur de service	Le fournisseur saisit le NPI de la carte fID (cette étape peut être automatisée) et demande une authentification biométrique en sélectionnant la partie du corps à scanner (visage, empreinte digitale)
Poser la partie du corps à scanner devant la lecture	Fournisseur de service	Le fournisseur aide le citoyen à poser la partie de son corps sélectionnée devant le scanner biométrique
Lancer l'opération de lecture de la donnée biométrique	Système d'identification	Le scanner biométrique lit les données de la partie du corps sélectionnée pour valider l'identité du citoyen via le système d'identification
NPI trouvable ?	Système d'identification	Le système vérifie si le NPI correspond à celui enregistré sur la carte fID existe
Qualité de la prise acceptable ?	Système d'identification	Le système doit proposer une prise de qualité suffisante pour que l'authentification soit réalisable
Chercher le template des données biométriques par le NPI	Système d'identification	Le système cherche le template des données biométriques correspondant au NPI du citoyen dans la base de données
Comparaison 1:1 de la biométrie	Système d'identification	Le système compare les données biométriques récupérées à celles enregistrées dans la base de données pour vérification
Envoyer le résultat de la requête	Système d'identification	Le système envoie le résultat de la requête pour valider l'authentification
Accorder le service demandé	Fournisseur de service	Si l'authentification est validée, le fournisseur accorde le service demandé au citoyen

Tableau 25 : Tableau descriptif du processus d'authentification par carte fID

6.3.2 Authentification par Mobile ID + biométrie ou PIN

Le citoyen a la possibilité de se rendre en personne chez un fournisseur de services avec sa son mobile ID. Tout d'abord, le fournisseur doit scanner le QR code présent sur son téléphone afin de vérifier son authenticité grâce à l'application de vérification des identités. Une fois que l'authenticité du mobile ID est confirmée, le fournisseur saisit le Numéro d'Identification Personnel (NPI) affiché dans le QR code (cette étape peut être automatisée). Ensuite, il demande une authentification, qui peut être réalisée soit par PIN, soit par une méthode biométrique, telle qu'une vérification du visage ou de l'empreinte, pour valider l'identité du citoyen.

Après avoir authentifié le citoyen avec succès, le fournisseur peut alors procéder à la demande de service du citoyen.

Ci-dessous la figure qui détaille les étapes en cas d'authentification par mobile ID et biométrie/PIN

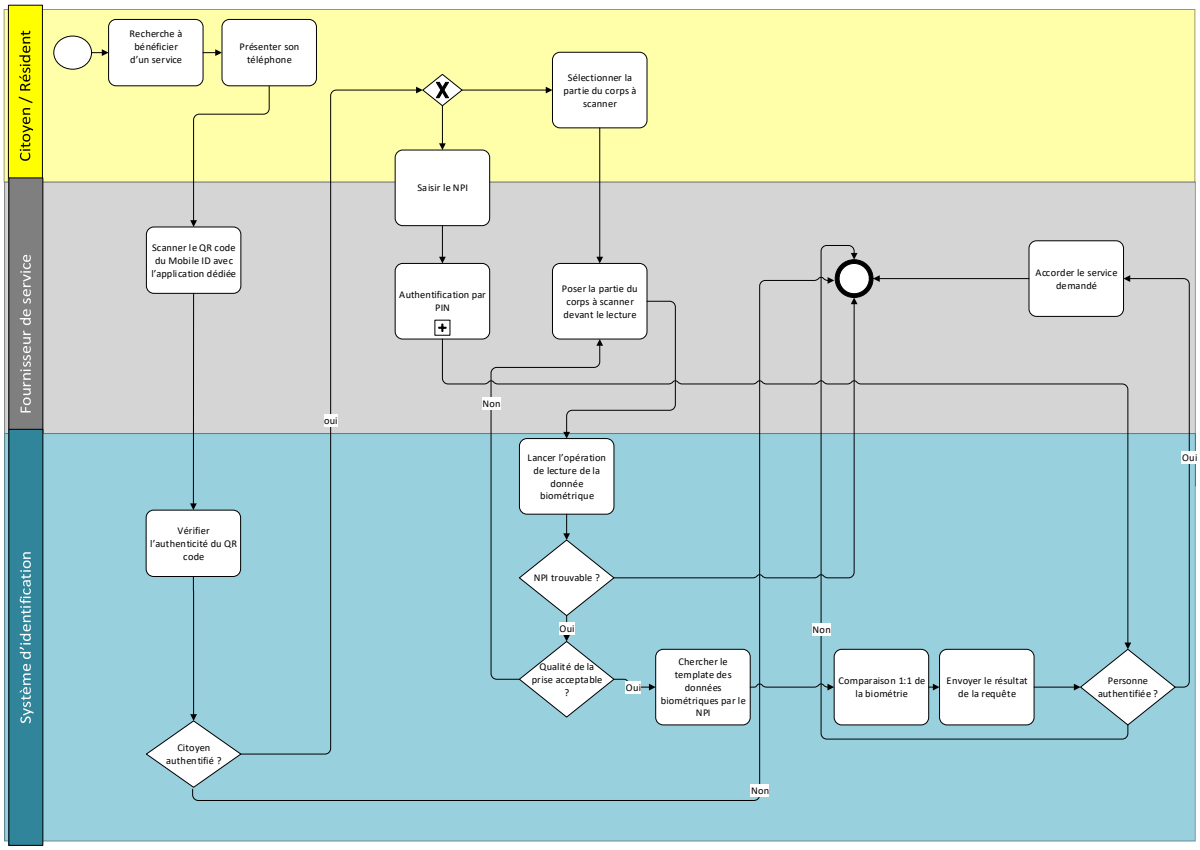


Figure 26 : Processus d'authentification par Mobile ID

Ci-dessous un tableau qui récapitule les étapes décrites plus haut en lien avec le processus d'authentification par mobile ID.

Etape	Responsable/Système	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident se déplace physiquement chez un fournisseur de service pour bénéficier d'un service.
Présenter son téléphone	Citoyen / résident	Le citoyen se présente physiquement avec son téléphone
Scanner le QR code du mobile ID avec l'application dédiée	Fournisseur de service	Le fournisseur utilise une application dédiée pour scanner le QR code présent sur la carte fID.
Vérifier l'authenticité du QR code	Système d'identification	Le système d'identification vérifie l'authenticité du QR code scanné
Citoyen authentifié ?	Système d'identification	Le système d'identification confirme l'authenticité de la carte fID
Saisir le NPI	Fournisseur de service	Le fournisseur saisit le NPI du citoyen concerné (cette étape peut être automatisée)

Etape	Responsable/Système	Description
Option1 : Authentification par PIN	Fournisseur de service	Sous processus « Authentification par PIN »
Option 2 : Poser la partie du corps à scanner devant la lecture	Fournisseur de service	Le fournisseur aide le citoyen à poser la partie de son corps sélectionnée devant le scanner biométrique
Lancer l'opération de lecture de la donnée biométrique	Système d'identification	Le scanner biométrique lit les données de la partie du corps sélectionnée pour valider l'identité du citoyen via le système d'identification
NPI trouvable ?	Système d'identification	Le système vérifie si le NPI correspond à celui enregistré sur la carte fID existe
Qualité de la prise acceptable ?	Système d'identification	Le système doit proposer une prise de qualité suffisante pour que l'authentification soit réalisable
Chercher le template des données biométriques par le NPI	Système d'identification	Le système cherche le template des données biométriques correspondant au NPI du citoyen dans la base de données
Comparaison 1:1 de la biométrie	Système d'identification	Le système compare les données biométriques récupérées à celles enregistrées dans la base de données pour vérification
Envoyer le résultat de la requête	Système d'identification	Le système envoie le résultat de la requête pour valider l'authentification
Accorder le service demandé	Fournisseur de service	Si l'authentification est validée, le fournisseur accorde le service demandé au citoyen

Tableau 26 : Tableau descriptif du processus d'authentification par Mobile ID

6.4 Citoyen hors ligne : Authentification hors ligne à 3 facteurs

En raison de l'importance cruciale du service demandé, le fournisseur de services peut imposer une authentification à trois facteurs pour renforcer la sécurité. Dans ce cas, le citoyen doit se présenter en personne, hors ligne (c'est-à-dire, sans être connecté à Internet), en fournissant trois facteurs

d'authentification. Il peut choisir soit de présenter sa carte fID accompagnée de sa biométrie et d'un (OTP), soit de présenter son Mobile ID avec ses données biométriques et son code PIN.

Ci-dessous la figure qui détaille les étapes en cas d'authentification à 3 facteurs hors ligne.

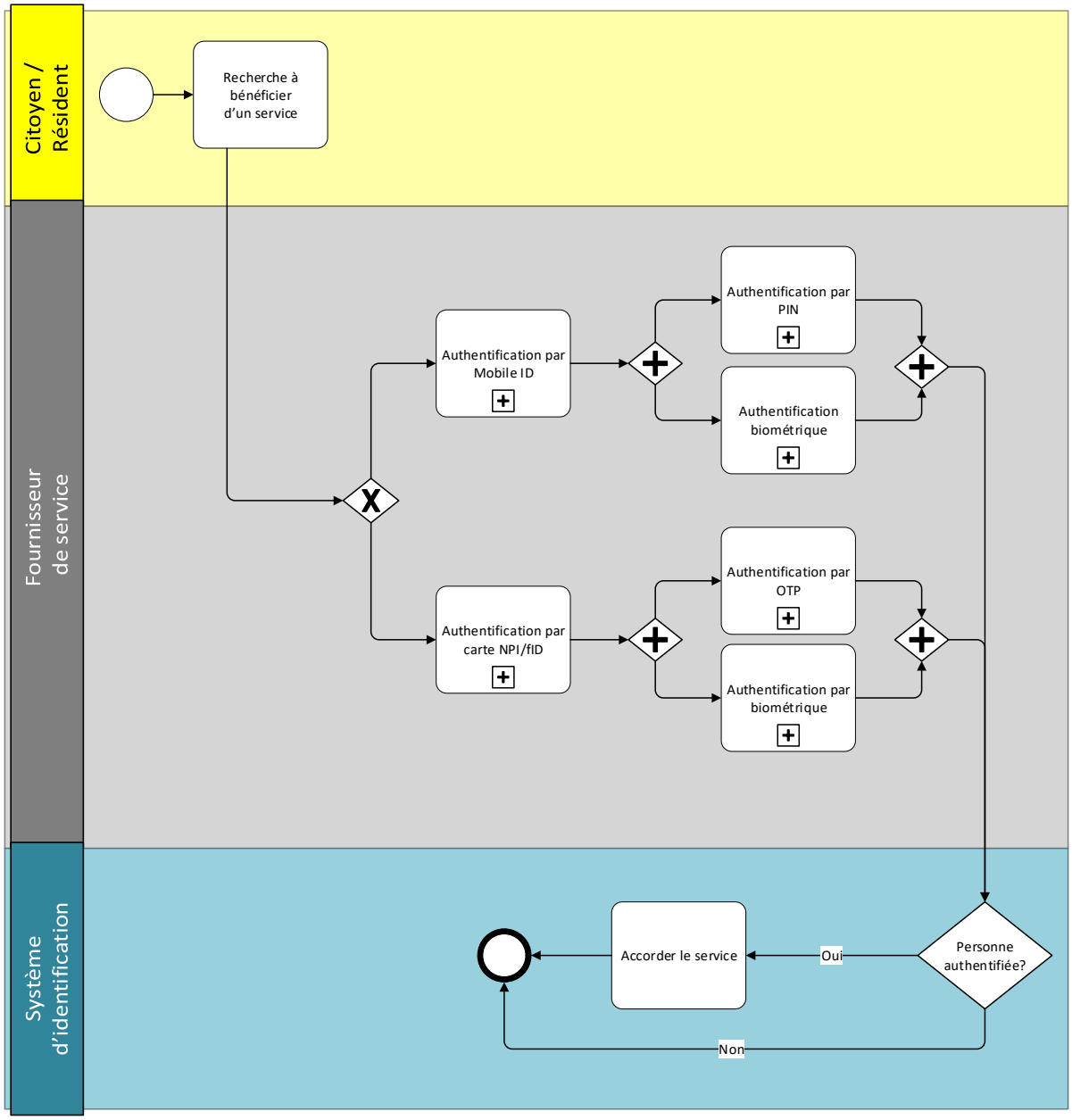


Figure 27 : Processus d'authentification multifactorielle hors ligne

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus d'authentification MFA hors ligne.

Etape	Responsable	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident cherche à bénéficier d'un service chez un fournisseur de service public ou privé

option 1 : Présenter sa carte fID	Citoyen / résident	Le citoyen/résident présente sa carte fID au fournisseur de service pour s'authentifier
S'authentifier par OTP	Citoyen / résident	Le citoyen/résident s'authentifie moyennant un OTP envoyé par SMS que le fournisseur de service doit saisir pour valider l'identité du citoyen/résident
S'authentifier par ses données biométriques	Citoyen / résident	Le citoyen /résident s'authentifie moyennant son empreinte ou son visage
Option 2 : Présenter son mobile ID	Citoyen / résident	Le citoyen présente son Mobile ID
S'authentifier par PIN	Citoyen / résident	Le citoyen/résident saisir son PIN pour valider son identité
S'authentifier par ses données biométriques	Citoyen / résident	Le citoyen /résident s'authentifie moyennant son empreinte ou son visage
Vérifier l'identité du citoyen	Système d'identification	Le système d'identification vérifie l'authenticité des données fournies. Si les données saisies sont authentiques, l'étape « Accorder un service » sera déclenché.

Tableau 27 : Tableau descriptif du processus d'authentification hors ligne à 3 facteurs

6.5 Fournisseur de service hors ligne : Authentification par QR code

Avant d'être diffusé, chaque QR code est signé numériquement à l'aide d'une clé privée et une clé asymétrique publique (paire de clés publique/privée) générées par l'annuaire de l'état via le PKI (géré par l'ASIN).

- Clé Privée : est confidentielle et intégrée au QR code détenu par le citoyen/résident.
- Clé Publique : correspondante à la clé privée est distribuée et reconnaissable par l'application de vérification des identités.

L'application de vérification des identités requiert une connexion Internet à l'installation (nécessaire pour le premier téléchargement des certificats depuis l'annuaire de l'état pour la validation du QR code) puis à chaque fois que l'application détecte une connexion internet, elle procède automatiquement à la mise à jour des certificats (un mécanisme de mise à jour incrémentielle où seulement les changements récents sont téléchargés et non la base de données complète).

L'application peut donc fonctionner en deux modes :

- mode offline : ce mode se base sur le dernier certificat téléchargé pour valider le QR code du certificat scanné. Pendant l'opération, un message attire l'attention sur le fait que l'application est en mode offline et que les informations affichées peuvent avoir été modifiées et que pour avoir les dernières informations à jour, il est préférable de se connecter à Internet.

- mode online : en mode online l'application interroge directement la base de données et valide les certificats en temps réel.

Cette partie concerne le mode offline, lorsqu'un fournisseur de service scanne le QR code, l'application utilise la clé publique pour vérifier la signature numérique. En cas de succès de cette vérification, indiquant la compatibilité entre la clé publique et la clé privée présente sur le QR code, l'intégrité des données et l'authenticité du QR code sont confirmées.

Après avoir scanné le QR code, les informations liées à l'identité du titulaire de la carte seront affichées :

- Informations personnelles : Nom, prénom, date de naissance, lieu de naissance, genre, etc.
- Le numéro NPI
- Données biométriques : Photo du citoyen

Le fournisseur de service peut voir et vérifier les données affichées sur l'application (notamment la comparaison entre la photo affichée et le visage de la personne présente).

Ci-dessous le processus d'authentification modélisé

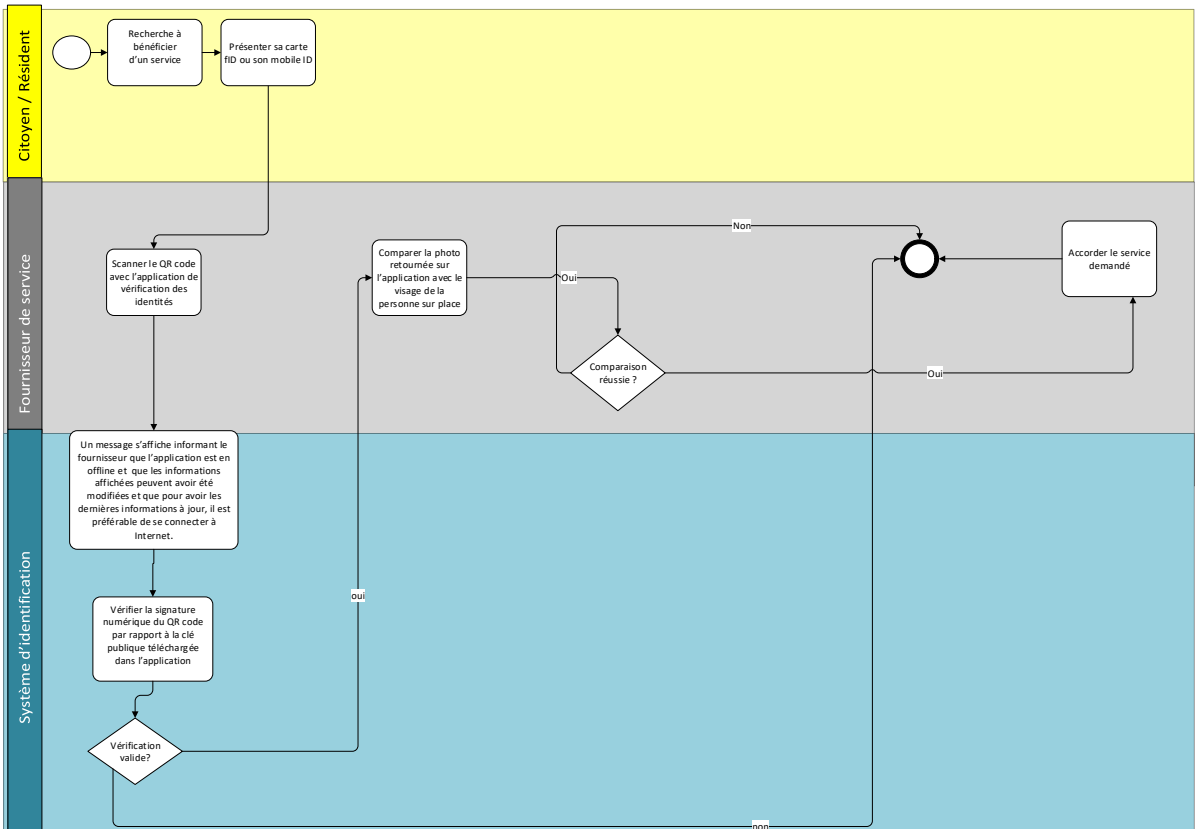


Figure 28 : Processus d'authentification : fournisseur de service hors ligne

Le tableau ci-dessous récapitule les étapes modélisées dans la figure ci-dessus

Etape	Responsable/Système	Description
Chercher à bénéficier d'un service	Citoyen / résident	Le citoyen/résident se déplace physiquement chez un fournisseur de service pour bénéficier d'un service.
Présenter son mobile ID ou sa carte fID	Citoyen / résident	Le citoyen se présente physiquement avec sa carte fID ou son Mobile ID
Scanner le QR code du mobile ID avec l'application de vérification des identités	Fournisseur de service	Le fournisseur n'ayant pas accès à Internet vérifier utilise l'application de vérification des identités
Un message informatif s'affiche sur l'écran	Système d'identification	Un message attire l'attention sur le fait que l'application est en mode offline et que les informations affichées peuvent avoir été modifiées et que pour avoir les dernières informations à jour, il est préférable de se connecter à Internet.
Vérifier la signature numérique du QR code par rapport à la clé publique téléchargée dans l'application	Système d'identification	Le système d'identification vérifie l'authenticité du QR code scanné et ceci en comparant la clé privée du QR code avec la clé publique téléchargée en local sur l'application
Citoyen authentifié ?	Système d'identification	Le système d'identification confirme l'authenticité du QR code
Comparer la photo retournée par le QR code avec le visage de la personne sur place	Fournisseur de service	Le fournisseur de service doit vérifier et comparer la photo retournée par le QR code et le visage de la personne présente sur place.
Comparaison réussie ?	Système d'identification	Le système vérifier si la comparaison des deux données biométriques (photo du citoyen) s'est effectuée avec succès ou pas
Accorder le service demandé	Fournisseur de service	Si l'authentification est validée, le fournisseur accorde le service demandé au citoyen

Tableau 28 : Tableau descriptif du processus d'authentification : fournisseur hors ligne

7 Processus de gestion de l'identité

7. Processus de gestion de l'identité

Les processus de gestion de l'identité détaillent les étapes que les citoyens/résidents doivent suivre sur le portail fID ou sur l'application mobile pour accéder à des services liés à leur identité, tels que :

- La révocation d'une identité virtuelle
- La révocation du mobile ID
- Le verrouillage/déverrouillage du NPI
- La réédition/édition d'un certificat NPI/fID
- La gestion du profil et suivi des mises à jour

7.1 Révocation d'un IDV

La révocation d'un IDV peut se faire de deux façons différentes.

- La première méthode sera par la création d'un nouveau IDV en suivant le processus détaillé dans 4.2, l'ancien IDV sera systématiquement révoqué
- La deuxième méthode sera une révocation standard à travers le portail fID ou l'application mobile en cliquant sur l'option « Révoquer un IDV », cette méthode est détaillée dans le processus ci-dessous.

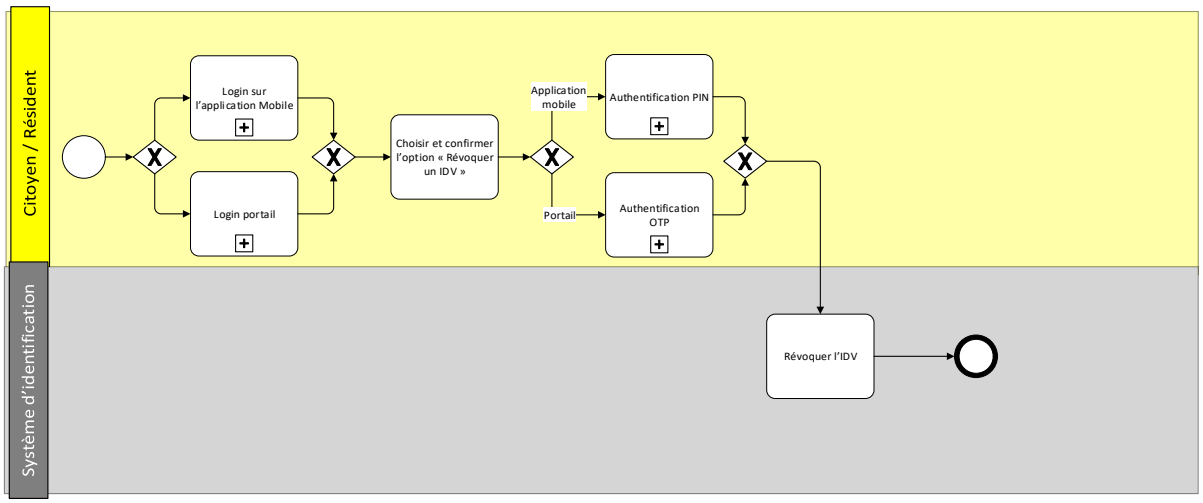


Figure 29 : Processus de révocation du IDV

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de révocation d'un IDV.

Etape	Responsable/Système	Description
Login sur l'application mobile	Citoyen / résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login portail	Citoyen / résident	
Choisir et confirmer l'option « Révoquer un IDV »	Citoyen / résident	Le citoyen/résident choisit le service de révocation de l'IDV et le confirme
Authentification PIN	Citoyen / résident	Dans le cas où le citoyen/résident utilise l'application mobile, il doit s'authentifier une autre fois en utilisant son PIN
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID, il doit s'authentifier une autre fois en utilisant un OTP qui sera envoyé à son numéro de téléphone déja enregistré dans la base de données RNPP.

Etape	Responsable/Système	Description
Révoquer l'IDV	Système d'identification	Pour finaliser le processus, le système d'identification révoque l'IDV du citoyen/résident

Tableau 29 : Tableau descriptif des étapes du processus de révocation d'un IDV

7.2 Révocation mobile ID

Le citoyen/résident est déconnecté systématiquement de l'application après 5 min d'inactivité sur ce compte mais peut se reconnecter au besoin avec son login.

Au cas où le citoyen/résident souhaite révoquer son mobile ID pour n'importe quelle raison à savoir le changement, l'inaccessibilité ou le vol du smartphone etc, deux possibilités sont envisagées et sont détaillées comme suit :

- Via le portail

Le citoyen/résident choisit le service « révoquer un mobile ID » de la rubrique services d'identité en précisant la raison pour la révocation, il saisit ensuite son mot de passe pour confirmer la révocation.

Le système envoie une notification par email et par SMS à la personne enregistrée pour lui informer que le mobile ID a été désactivé sur l'ancien appareil en spécifiant la marque et le modèle du smartphone.

- Via application mobile

Via l'application mobile installée sur le nouvel appareil, le citoyen/résident se connecte à son compte fID et demande d'activer le mobile ID sur ce nouvel appareil.

Après s'être connecté à l'application mobile (il sera alors automatiquement déconnecté de l'ancien appareil si la connexion est toujours active), le citoyen/résident peut activer le mobile ID sur le nouvel appareil qui récupérera automatiquement les informations du nouveau smartphone, opération qu'il devra confirmer en entrant un OTP.

Le système envoie une notification par email et par SMS à la personne enregistrée pour lui informer que le mobile ID a été activé sur le nouvel appareil et désactivé sur l'ancien appareil en spécifiant la marque et le modèle des deux appareils

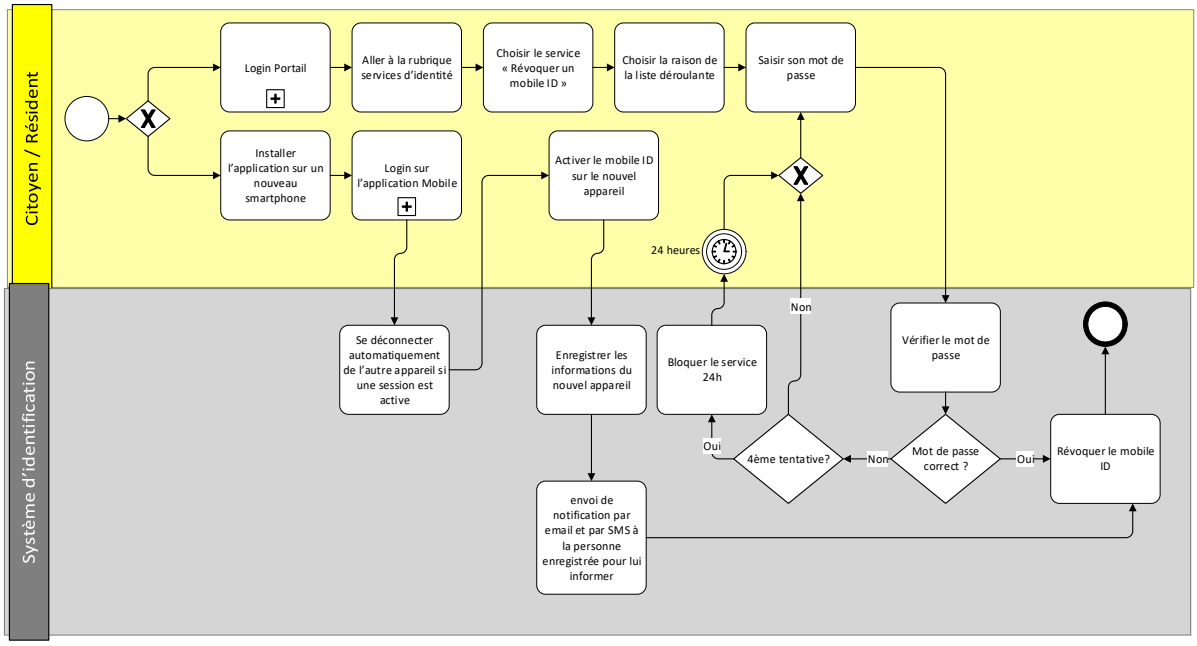


Figure 30 : Processus de révocation du mobile ID

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de révocation du mobile ID.

Etape	Responsable/Système	Description
Option 1 : avec le portail, Login portail	Citoyen / résident	Le citoyen/résident se connecte à son compte via le portail fID
Choisir le service « Révoquer un mobile ID »	Citoyen / résident	Le citoyen/résident choisit le service de révocation de mobile ID et le confirme
Choisir la raison de la liste déroulante	Citoyen / résident	Le citoyen/résident choisit la raison pour laquelle il veut révoquer son mobile ID
Saisir son mot de passe	Citoyen / résident	Le citoyen/résident s'authentifie à travers son mot de passe
Vérifier le mot de passe	Système d'identification	Le système vérifie si le mot de passe est correct
Bloquer le service 24 heures	Système d'identification	Si le mot de passe n'est pas correct au bout de la 3ème tentative, le service sera bloqué pour 24 heures dans la 4ème tentative
Option 2 : via l'application mobile : Installer l'application sur un nouveau smartphone	Citoyen / résident	Dans le cas où le citoyen/résident à déjà un compte mobile ID actif sur un smartphone et il a un besoin de transférer le compte à un autre appareil (à noter que le compte mobile ID ne peut être actif que sur un seul appareil), il doit installer l'application mobile ID sur le nouvel appareil avant.
Login sur l'application mobile	Citoyen / résident	Le citoyen/résident se connecte sur l'application mobile installée sur le nouvel appareil
Déconnecter le citoyen automatiquement des	Système d'identification	Le système déconnecte automatiquement les sessions actives sur d'autres appareils.

Etape	Responsable/Système	Description
autres sessions actives		
Enregistrer les informations du nouveau smartphone	Le citoyen	Le nouveau smartphone (IMEI) est enregistré à la place de l'ancien smartphone
Informer la personne enregistrée du changement	Système d'identification	Le système envoie une notification par email et par SMS à la personne enregistrée pour lui informer que le mobile ID a été activé sur le nouvel appareil et désactivé sur l'ancien appareil en spécifiant la marque et le modèle des deux appareils

Tableau 30 : Tableau descriptif des étapes du processus de révocation du mobile ID

7.3 Edition/Réédition du certificat fID/NPI

7.3.1 Edition/Réédition du certificat fID/NPI en ligne

Le citoyen/résident a la possibilité de demander l'édition de son certificat fID/NPI afin de pouvoir la télécharger ou encore la réédition de son certificat fID/NPI, que ce soit depuis le portail fID ou l'application mobile, pour diverses raisons telles que la perte du certificat NPI/fID, la mise à jour des informations liées à leur identité ou encore l'endommagement du certificat actuel. Pour effectuer cette réédition, le citoyen/résident doit fournir toutes les pièces administratives justifiant la nécessité de la mise à jour, lesquelles doivent être téléchargées dans le système d'identification. L'ANIP examine ces pièces pour vérifier la légitimité de la demande. En cas d'acceptation de la demande, le citoyen/résident doit s'acquitter des frais de renouvellement du certificat (tel que défini lors dans la stratégie de renouvellement des certificats fID). Une fois le paiement effectué, un nouveau certificat est généré et le QR code de l'ancien certificat est désactivé. Le citoyen/résident peut alors télécharger et utiliser le nouveau certificat fID.

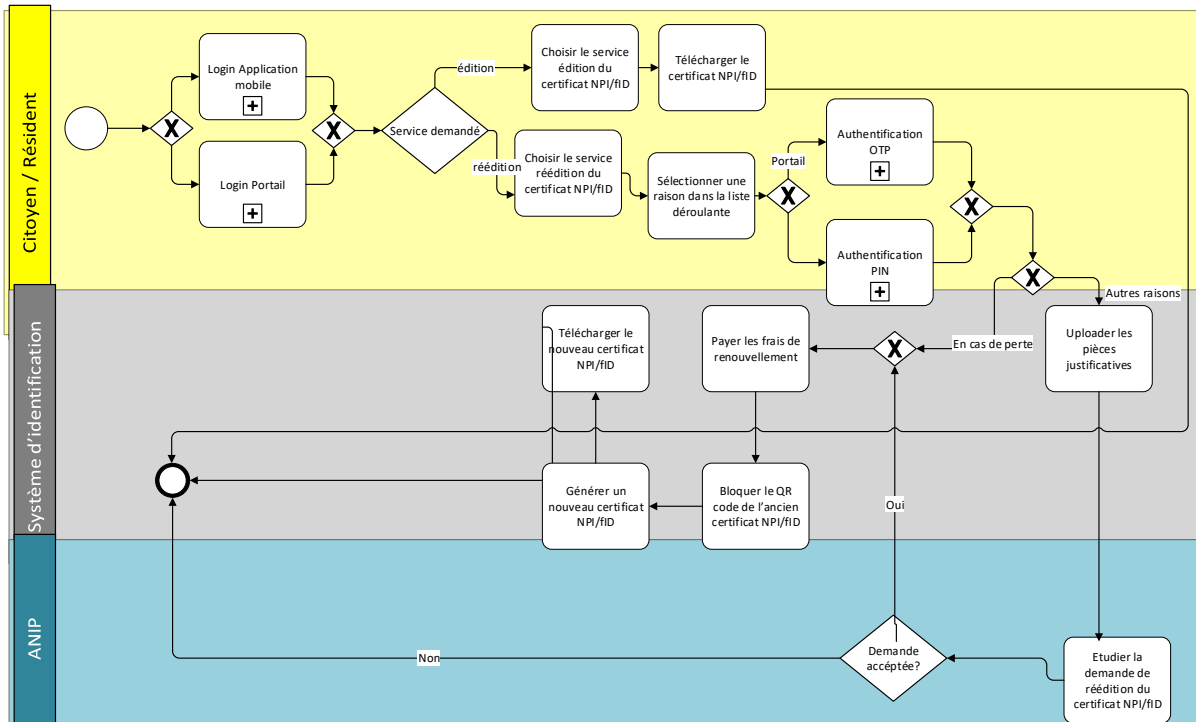


Figure 31 : Processus de réédition du certificat fID / NPI en ligne

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de réédition du certificat fID / NPI.

Etape	Responsable	Description
Login sur l'application mobile	Citoyen / résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login portail fID	Citoyen / résident	
Choisir le service de réédition ou édition du certificat NPI/fID	Citoyen / résident	Le citoyen/résident choisit le service de réédition ou édition du certificat NPI/fID
Si le service choisi est « édition du certificat NPI/fID »	Citoyen / résident	le citoyen/résident télécharge son certificat NPI/fID
Si le service choisi « réédition du certificat NPI/fID », Sélectionner une raison dans la liste déroulante	Citoyen / résident	Le citoyen/résident sélectionne une raison. Ces raisons peuvent être : • La perte du certificat NPI/fID • Autres raisons comme : Mise à jour des données sur le certificat NPI/fID, Certificat actuel défectueux, etc
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID pour demander le service, il doit s'authentifier par OTP
Authentification PIN	Citoyen / résident	Dans le cas où le citoyen/résident utilise l'application mobile pour demander le service, il doit s'authentifier en saisissant son PIN
Payer les frais de renouvellement	Citoyen / résident	Le citoyen/résident paie les frais de renouvellement en utilisant le mobile paiement ou une carte bancaire

Etape	Responsable	Description
Uploader les pièces justificatives	Citoyen / résident	Le citoyen/résident upload les documents nécessaires pour justifier la demande de réédition
Etudier la demande de réédition du certificat NPI/fID	ANIP	L'ANIP traite la demande en déterminant sa légitimité
Bloquer le QR code de l'ancien certificat NPI/fID	Système d'identification	Après l'acceptation de la demande de réédition du certificat NPI/fID, la première étape est de bloquer le QR code de l'ancien certificat pour empêcher toute tentative d'authentification
Générer d'un nouveau certificat NPI/fID	Système d'identification	Le système d'identification génère le nouveau certificat avec la mise à jour des informations demandées
Télécharger le nouveau certificat fID	Citoyen / résident	Le citoyen/résident peut télécharger le nouveau certificat via l'application mobile ou le portail fID

Tableau 31 : Tableau descriptif du processus de réédition du certificat fID / NPI

7.3.2 Réédition du certificat fID/NPI hors ligne

Le citoyen/résident a la possibilité de demander une réédition de son certificat fID/NPI en mode hors ligne pour diverses raisons telles que la perte du certificat NPI/fID, la mise à jour des informations liées à leur identité ou encore l'endommagement du certificat actuel. Pour effectuer cette réédition, le citoyen/résident doit se déplacer ver l'ANIP et fournir toutes les pièces administratives justifiant la nécessité de la mise à jour. L'ANIP examine ces pièces pour vérifier la légitimité de la demande. En cas d'acceptation de la demande, le citoyen/résident doit s'acquitter des frais de renouvellement du certificat (tel que défini lors dans la stratégie de renouvellement des certificats fID). Une fois le paiement effectué, un nouveau certificat est fourni au citoyen/résident et le QR code de l'ancien certificat est désactivé.

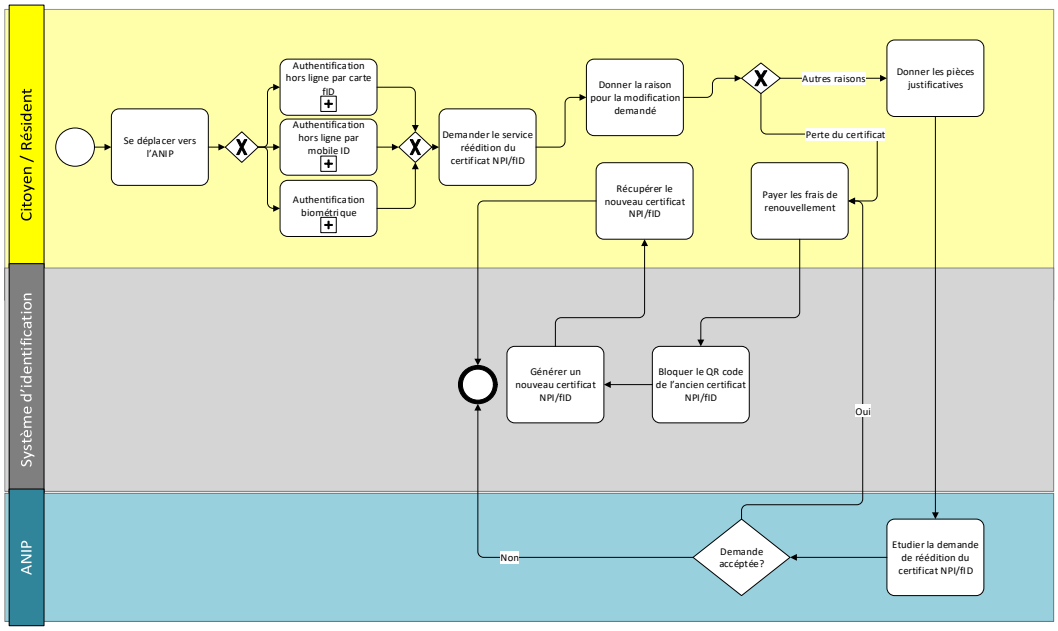


Figure 32 : Processus de réédition du certificat fID/NPI hors ligne

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de réédition du certificat fID / NPI en mode hors ligne.

Etape	Responsable	Description
Se déplacer vers l'ANIP	Citoyen / résident	Le citoyen/résident de déplace vers l'ANIP
Authentification hors ligne par carte fID	Citoyen / résident	Sous processus Authentification hors ligne par carte fID
Authentification hors ligne par mobile ID	Citoyen / résident	Sous processus Authentification hors ligne par mobile ID
Authentification biométrique	Citoyen / résident	Sous processus Authentification biométrique
Demander le service réédition du certificat NPI/fID	Citoyen / résident	Le citoyen/résident demande le service de réédition du certificat NPI/fID
Donner une raison dans la liste déroulante	Citoyen / résident	Le citoyen/résident sélectionne une raison. Ces raisons peuvent être : • La perte du certificat NPI/fID • Autres raisons comme : Mise à jour des données sur le certificat NPI/fID, Certificat actuel défectueux, etc
Donner les pièces justificatives	Citoyen / résident	Le citoyen/résident fournit les pièces justificatives et/ou les documents nécessaires pour justifier la demande de réédition
Payer les frais de renouvellement	Citoyen / résident	Le citoyen/résident paie les frais de renouvellement en utilisant le mobile paiement ou une carte bancaire
Etudier la demande de réédition du certificat NPI/fID	ANIP	L'ANIP traite la demande en déterminant sa légitimité
Bloquer le QR code de l'ancien certificat NPI/fID	Système d'identification	Après l'acceptation de la demande de réédition du certificat NPI/fID, la première étape est de bloquer le QR code de l'ancien certificat pour empêcher toute tentative d'authentification
Générer d'un nouveau certificat NPI/fID	Système d'identification	Le système d'identification génère le nouveau certificat avec la mise à jour des informations demandées
Récupérer le nouveau certificat fID	Citoyen / résident	Le citoyen/résident récupère le nouveau certificat via l'application mobile ou le portail fID

Tableau 32 : Tableau descriptif du processus de réédition du certificat fID/NPI hors ligne

7.4 Mise à jour des données d'identification démographiques

7.4.1 Mise à jour des données d'identification démographiques en ligne

Le processus ci-dessous décrit les étapes à suivre si un citoyen/résident souhaite mettre à jour ses données d'identification tels que (Nom, Prénom, Genre, Date de naissance, Nationalité, Profession, Statut, etc).

La mise à jour peut se faire à partir du portail fID ou de l'application mobile, le citoyen/résident doit sélectionner le service "Mise à jour des données démographiques " et choisir les données à mettre à jour,

en fournissant les pièces justificatives appropriées. L'ANIP examinera la demande pour vérifier sa légitimité. Si la demande est approuvée, le système d'identification mettra à jour les informations dans la base de données RNPP, avec une synchronisation automatique prenant en charge la mise à jour de la base de données PostgreSQL. Si les informations mises à jour sont également affichées sur le certificat NPI/fID, le citoyen/résident peut demander la réédition d'un nouveau certificat en payant les frais de renouvellement, puis choisir le service de réédition du certificat NPI/fID, qui pourra être téléchargé par la suite.

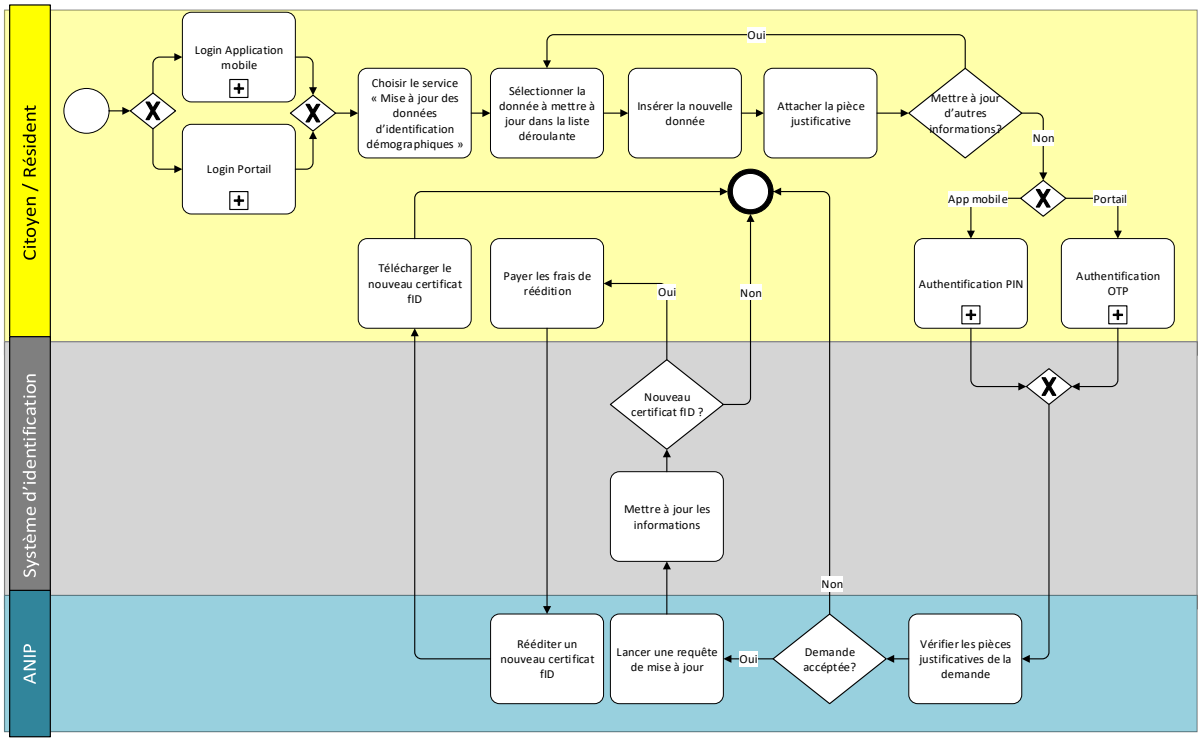


Figure 33 : Processus de mise à jour des données d'identification démographiques en ligne

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de mise à jour des données d'identification.

Etape	Responsable/Système	Description
Login sur application mobile	Citoyen / résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login portail fID	Citoyen / résident	
Choisir le service « Mise à jour des données d'identification démographiques »	Citoyen / résident	Le citoyen/résident choisit le service de mise à jour des données démographiques de la rubrique des services d'identité
Sélectionner la donnée à mettre à jour de la liste déroulante	Citoyen / résident	Le citoyen/résident choisit les données à mettre à jour de la liste déroulante. Ce processus concerne seulement les données démographiques
Insérer la nouvelle donnée	Citoyen / résident	Le citoyen/résident insère la nouvelle donnée à insérer

Etape	Responsable/Système	Description
Attacher les pièces justificatives	Citoyen / résident	Le citoyen/résident attache les documents nécessaires pour justifier la demande de mise à jour des données d'identification
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID pour demander le service, il doit s'authentifier par OTP
Authentification PIN	Citoyen / résident	Dans le cas où le citoyen/résident utilise l'application pour demander le service, il doit s'authentifier en saisissant son PIN
Vérifier les pièces justificatives de la demande	ANIP	L'ANIP vérifie la possibilité de mise à jour des données en fonction des justificatives présentées
Mettre à jour les informations	Système d'identification	Le système d'identification met à jour les informations dans la base de données RNPP. La synchronisation automatique prendra en charge la mise à jour de la base de données postgres
Payer les frais de réédition	Citoyen / résident	Dans le cas où l'information mise à jour est affichée sur le certificat NPI/fID, le citoyen/résident peut demander la réédition d'un nouveau certificat en payant les frais de renouvellement.
Rééditer un nouveau certificat NPI/fID	Système d'identification	Le citoyen/résident choisit le service de réédition d'un nouveau certificat NPI/fID et le confirme
Télécharger le nouveau certificat NPI/fID	Citoyen / résident	Le citoyen/résident choisit le service de téléchargement du nouveau certificat NPI/fID et le confirme

Tableau 33 : Tableau descriptif du processus de mise à jour des données d'identification

7.4.2 Mise à jour des données d'identification démographiques hors ligne

Le processus ci-dessous décrit les étapes à suivre si un citoyen/résident souhaite mettre à jour ses données d'identification tels que (Nom, Prénom, Genre, Date de naissance, Nationalité, Profession, Statut, etc) en mode hors ligne.

Le citoyen/résident doit se déplacer vers le centre d'enregistrement le plus proche et demander le service "Mise à jour des données d'identification démographiques" ensuite il renseigne les données qu'il souhaite mettre jour, en fournissant les pièces justificatives appropriées. L'agent examinera la demande pour vérifier sa légitimité. Si la demande est approuvée, L'agent mettra à jour les informations dans la base de données RNPP, avec une synchronisation automatique prenant en charge la mise à jour de la base de données PostgreSQL. Si les informations mises à jour sont également affichées sur le certificat NPI/fID, le citoyen/résident peut demander la réédition d'un nouveau certificat (mode hors ligne) en payant les frais de renouvellement, puis choisir le service de réédition du certificat NPI/fID, qui pourra être récupéré par la suite.

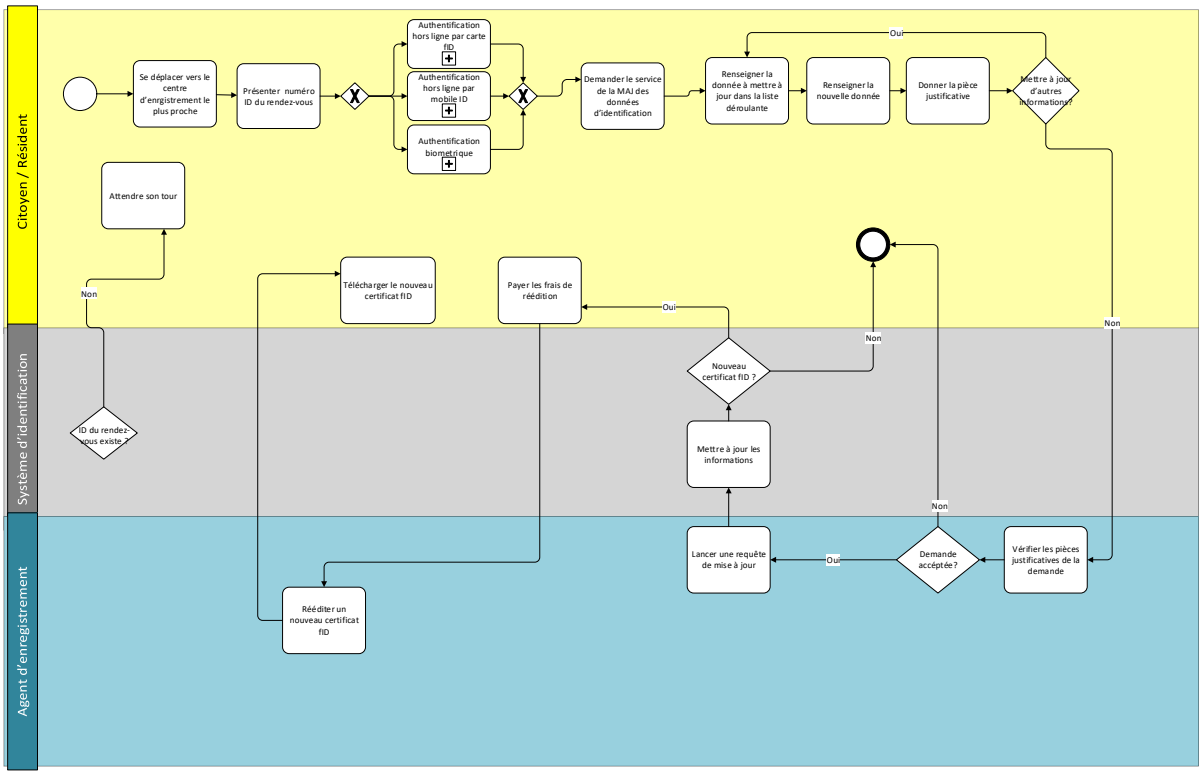


Figure 34 : Processus de mise à jour des données d'identification démographiques hors ligne

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de mise à jour des données d'identification en mode hors ligne.

Etape	Responsable/Système	Description
Se déplacer vers le centre d'enregistrement le plus proche	Citoyen / résident	Le citoyen/résident de déplace vers le centre d'enregistrement le plus proche
Option 1 : Authentification hors ligne par carte fID	Citoyen / résident	Le citoyen peut s'authentifier par carte fID + biométrie ou OTP
Option 2 : Authentification hors ligne par mobile ID	Citoyen / résident	Le citoyen peut s'authentifier par son Mobile ID + biométrie ou PIN
Option 3 : Authentification biométrique	Citoyen / résident	Le citoyen peut s'authentifier avec ses données biométriques (empreinte et visage)
Vérifier s'il a déjà pris un rendez-vous	Système d'identification	S'il n'a pas pris de rendez-vous le citoyen doit attendre son tour
Demander le service « Mise à jour des données d'identification démographiques »	Citoyen / résident	Le citoyen/résident demande le service de mise à jour des données démographiques de la rubrique des services d'identité
Renseigner la donnée à mettre à jour	Citoyen / résident	Le citoyen/résident renseigne les données à mettre à jour. Ce processus concerne seulement les données démographiques
Donner les pièces justificatives	Citoyen / résident	Le citoyen fournit toutes les pièces nécessaires qui justifie la mise à jour souhaitée

Etape	Responsable/Système	Description
Vérifier les pièces justificatives de la demande	Agent d'enregistrement	L'agent vérifie la possibilité de mise à jour des données en fonction des justificatives présentées
Lancer une requête de mise à jour	Agent d'enregistrement	L'agent lance une requête de mise à jour au système d'identification
Mettre à jour les informations	Système d'identification	Le système d'identification met à jour les informations dans la base de données RNPP. La synchronisation automatique prendra en charge la mise à jour de la base de données postgres
Payer les frais de réédition	Citoyen / résident	Dans le cas où l'information mise à jour est affichée sur le certificat NPI/fID, le citoyen/résident peut demander la réédition d'un nouveau certificat en payant les frais de renouvellement.
Rééditer un nouveau certificat NPI/fID	Système d'identification	Le citoyen/résident choisit le service de réédition d'un nouveau certificat NPI/fID et le confirme
Récupérer le nouveau certificat NPI/fID	Citoyen / résident	Le citoyen/résident récupère le nouveau certificat NPI/fID et le confirme

Tableau 34 : Tableau descriptif du processus de mise à jour des données d'identification démographiques hors ligne

7.5 Mise à jour des données biométriques

Ce processus donne la possibilité au citoyen/résident de mettre à jour ses données biométriques au besoin, et pour ce faire il doit se déplacer au centre d'enregistrement le plus proche et demander de mettre à jour ses biométries (visage ou empreinte).

Il est préférable pour éviter les temps d'attente de prendre un rendez-vous sur l'application mobile ou le portail de la même façon que la prise du rendez-vous pour le pré-enregistrement en précisant le motif qui est la mise à jour des données biométriques.

Ci-dessous le process qui décrit les étapes à suivre pour mettre à jour les données biométriques.

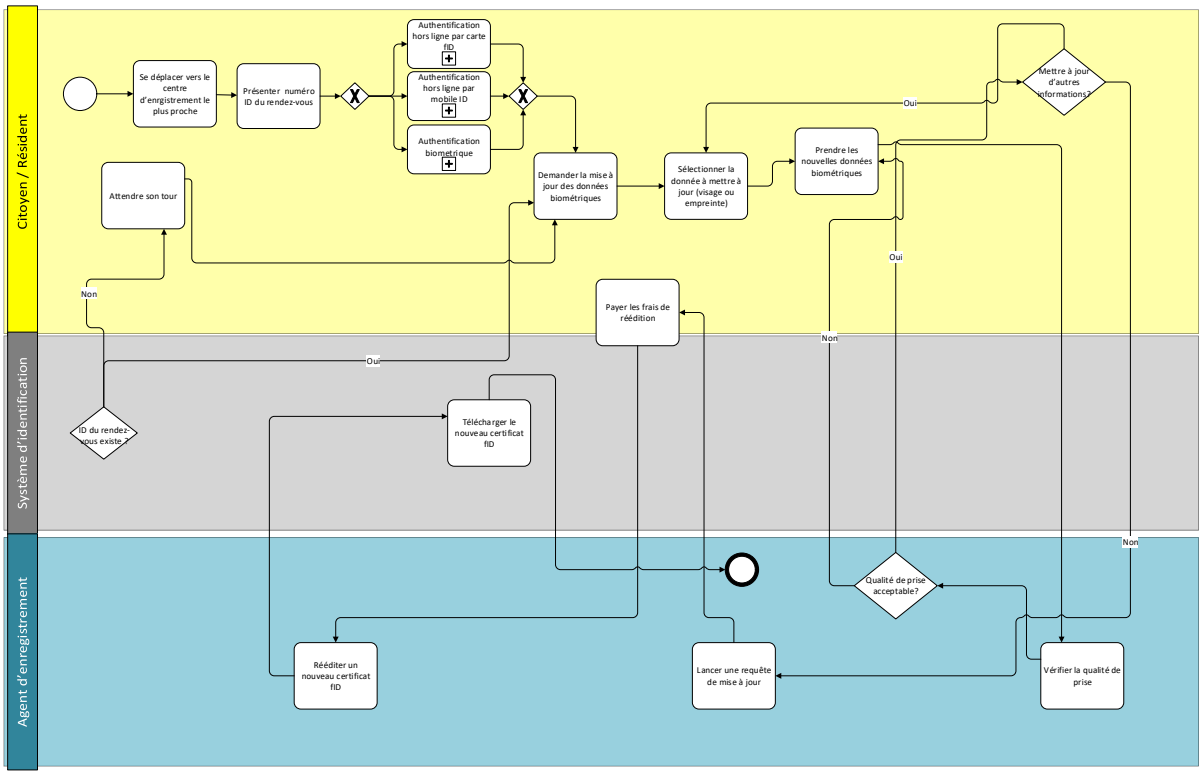


Figure 35 : Processus de mise à jour des données biométriques

Ci-dessous le tableau avec les étapes détaillées

Etape	Responsable/Système	Description
Se déplacer vers le centre d'enregistrement le plus proche	Citoyen / résident	Le citoyen/résident de déplace vers le centre d'enregistrement le plus proche
Option 1 : Authentification hors ligne par carte fID	Citoyen / résident	Le citoyen peut s'authentifier par carte fID + biométrie ou OTP
Option 2 : Authentification hors ligne par mobile ID	Citoyen / résident	Le citoyen peut s'authentifier par son Mobile ID + biométrie ou PIN
Option 3 : Authentification biométrique	Citoyen / résident	Le citoyen peut s'authentifier avec ses données biométriques (empreinte et visage)
Vérifier si le citoyen a déjà pris un rendez-vous ou pas	Système d'identification	Si le citoyen n'a pas pris de rendez-vous il devra attendre son tour
Demander le service « Mise à jour des données biométriques »	Citoyen / résident	Le citoyen/résident demande le service de mise à jour des données biométriques de la rubrique des services d'identité
Renseigner la donnée à mettre à jour	Citoyen / résident	Le citoyen/résident renseigne les données à mettre à jour. Ce processus concerne seulement les données démographiques

Etape	Responsable/Système	Description
Valider la qualité de prise de données biométrique mise à jour	Système d'identification	Le système valide la qualité de prise de données avant de poursuivre à la mise à jour
Lancer une requête de mise à jour	Agent d'enregistrement	L'agent lance une requête de mise à jour au système d'identification
Mettre à jour les informations	Système d'identification	Le système d'identification met à jour les informations dans la base de données RNPP. La synchronisation automatique prendra en charge la mise à jour de la base de données PostgreSQL
Payer les frais de réédition	Citoyen / résident	Dans le cas où l'information mise à jour est affichée sur le certificat NPI/fID, le citoyen/résident peut demander la réédition d'un nouveau certificat en payant les frais de renouvellement.
Rééditer un nouveau certificat NPI/fID	Système d'identification	Le citoyen/résident choisit le service de réédition d'un nouveau certificat NPI/fID et le confirme
Récupérer le nouveau certificat NPI/fID	Citoyen / résident	Le citoyen/résident récupère le nouveau certificat NPI/fID et le confirme

Tableau 35 : Tableau descriptif du processus de mise à jour des données biométriques

7.6 Verrouillage / Déverrouillage du NPI

Le processus ci-dessous consiste au verrouillage de l'utilisation du NPI pour des opérations d''authentification.

Le citoyen/résident peut verrouiller son NPI pour plusieurs raisons de sécurité telle que la perte de sa carte fID, la perte de son appareil mobile, le soupçon d'activités illicites avec son identité, etc.

Ceci est possible à travers le service « verrouillage du NPI » présent dans le portail fID et dans l'application mobile, le citoyen/résident doit préciser le motif de cette action de verrouillage.

Un message sera affiché au citoyen/résident pour l'informer que le verrouillage du NPI ne peut pas être à vie et que l'ANIP pourra le déverrouiller en cas de besoin

Ci-dessous le processus illustrant les étapes à suivre pour verrouiller le NPI.

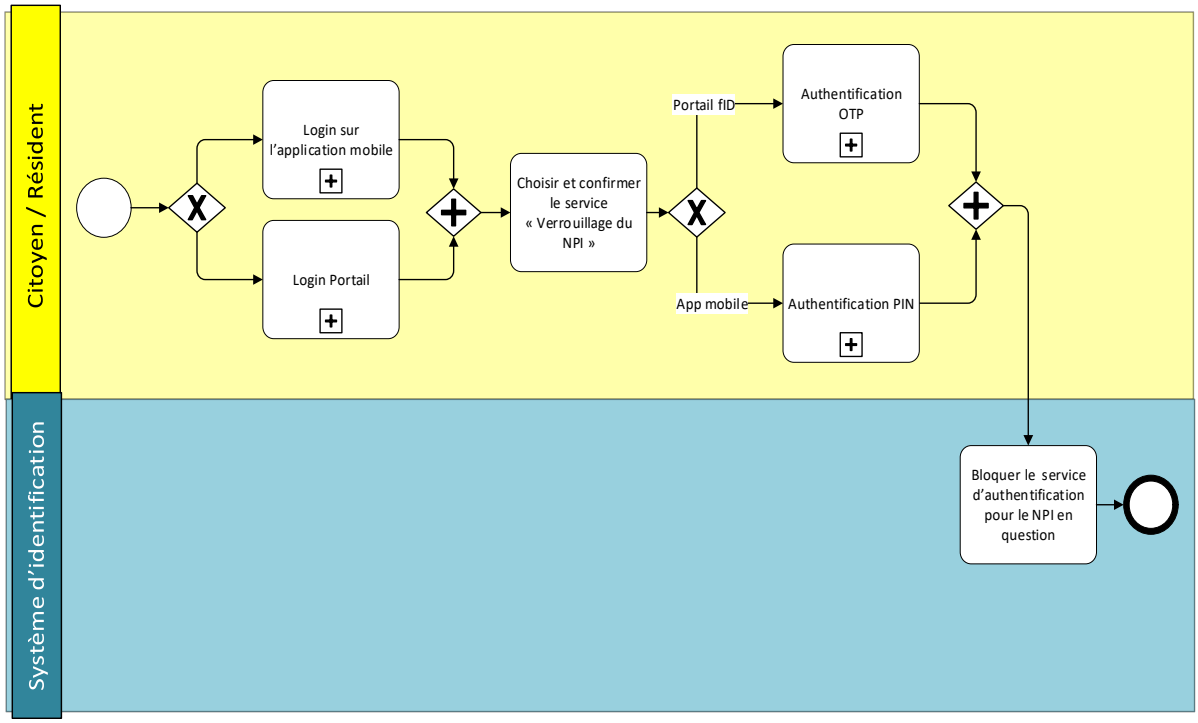


Figure 36 : Processus de verrouillage de NPI

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de verrouillage du NPI.

Etape	Responsable/Système	Description
Login application mobile	Citoyen/Résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login Portail	Citoyen/Résident	
Choisir le motif du verrouillage	Citoyen/Résident	Le citoyen/résident choisit le motif du verrouillage.
Choisir et confirmer le service « verrouillage du NPI »	Citoyen/Résident	Le citoyen/résident choisit le service « verrouillage du NPI » et le confirme
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID pour demander le service, il doit s'authentifier par OTP
Authentification PIN	Citoyen / résident	Dans le cas où le citoyen/résident utilise l'application mobile pour demander le service, il doit s'authentifier en saisissant son PIN
Message affiché	Système d'identification	Un message sera affiché au citoyen/résident pour lui indiquer que le verrouillage du NPI ne peut être permanent, et que l'ANIP peut le désactiver en cas de nécessité.
Bloquer le service d'authentification pour le NPI en question	Système d'identification	Pour finaliser le processus, le système d'identification bloque l'authentification pour le NPI.

Tableau 36 : Tableau descriptif du processus de verrouillage du NPI

Le NPI peut être déverrouillé grâce au service « Déverrouillage du NPI » qui est présent dans le portail fID et dans l'application mobile et qui est décrit dans la figure ci-dessous.

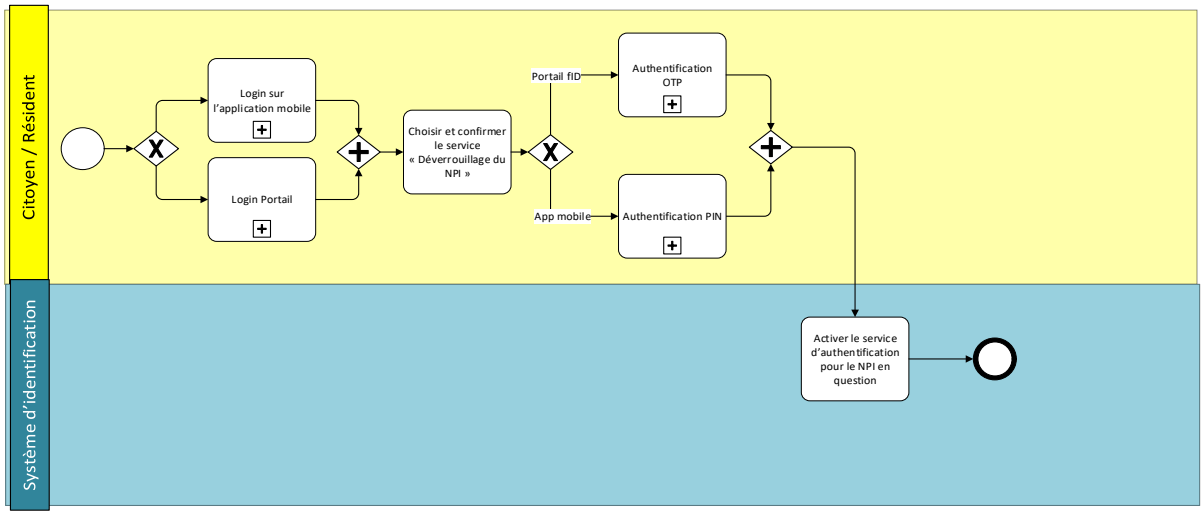


Figure 37 : Processus de déverrouillage du NPI

Ci-dessous un tableau qui récapitule les étapes décrites ci-dessus et liées au processus de déverrouillage du NPI.

Etape	Responsable/Système	Description
Login l'application mobile	Citoyen/Résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Login Portail	Citoyen/Résident	
Choisir et confirmer le service « Déverrouillage du NPI »	Citoyen/Résident	Le citoyen/résident choisit le service « Déverrouillage du NPI » puis le confirme
Authentification OTP	Citoyen / résident	Dans le cas où le citoyen/résident utilise le portail fID pour demander le service, il doit s'authentifier par OTP
Authentification PIN	Citoyen / résident	Dans le où le citoyen/résident utilise l'application mobile pour demander le service, il doit s'authentifier en saisissant son PIN
Débloquer le service d'authentification pour le NPI en question	Système d'identification	Pour finaliser le processus, le système d''identification réactive l''authentification pour le NPI.

Tableau 37 : Tableau descriptif du processus de déverrouillage de NPI

7.7 Gestion du profil et suivi des mises à jour

Le citoyen/résident a la possibilité de gérer son profil sur l'application mobile et sur le portail fID grâce à la fonctionnalité « Gestion du profil et suivi des mises à jour ».

Cette fonctionnalité donne la possibilité au citoyen/résident de mettre à jour son PIN et son mot de passe sur le portail des services publics et sur l'application mobile et de consulter l'historique des transactions effectuées sur son ID. Cet historique peut inclure les mises à jour des informations d'identification, les opérations d'authentifications, etc.

Ci-dessous le processus qui décrit les étapes à suivre pour la gestion du profil et le suivi des mises à jour.

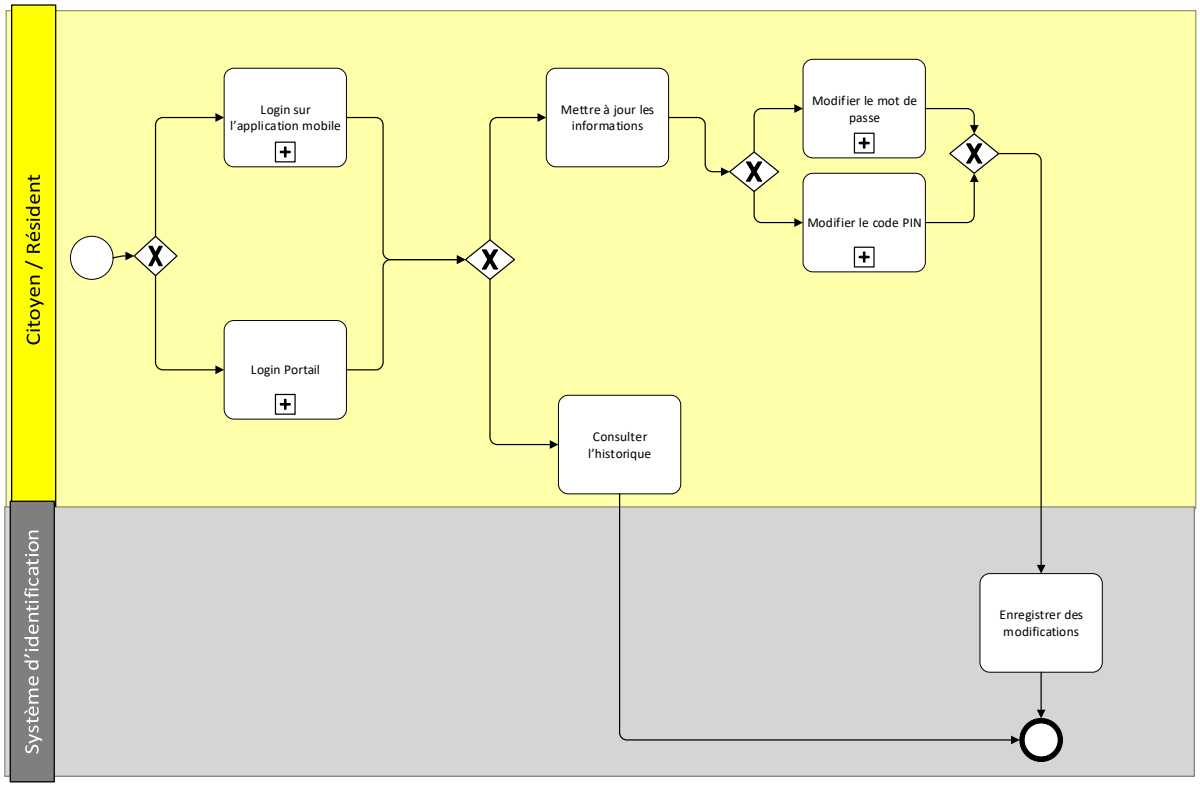


Figure 38 : Processus de gestion du profil et suivi des mises à jour

Ci-dessous le tableau descriptif des étapes pour la gestion du profil et le suivi des mises à jour

Etape	Responsable	Description
Lancer l'application	Citoyen / résident	Le citoyen/résident lance l'application installée sur son smartphone ou bien sur le portail
Option 1 : Mettre à jour les informations	Citoyen / résident	Le citoyen/résident choisit le service « mettre à jour les informations »
Modifier le mot de passe	Citoyen / résident	Le citoyen/résident a la possibilité de mettre à jour son mot de passe
Modifier le PIN	Citoyen / résident	Le citoyen/résident a la possibilité de mettre à jour son PIN
Enregistrer les modifications	Citoyen / résident	Le système d'identification enregistre les données modifiées

Etape	Responsable	Description
Option2 : Consulter l'historique	Citoyen / résident	Le citoyen/résident a la possibilité de choisir le service « consultation de l'historique » pour consulter l'historique des transactions réalisées sur son ID.

Tableau 38 : Tableau descriptif du processus de gestion du profil et suivi des mises à jour

7.7.1 Mise à jour du mot de passe

Afin de gérer au mieux son profil et dans un souci d'optimisation des procédures sécuritaires du compte du citoyen/résident dans l'application mobile ou dans le portail fID, le citoyen/résident aura la possibilité de mettre à jour son mot de passe au besoin.

Ci-dessous le processus qui décrit les étapes à suivre pour mette à jour le mot de passe sur le portail fID et sur l'application mobile.

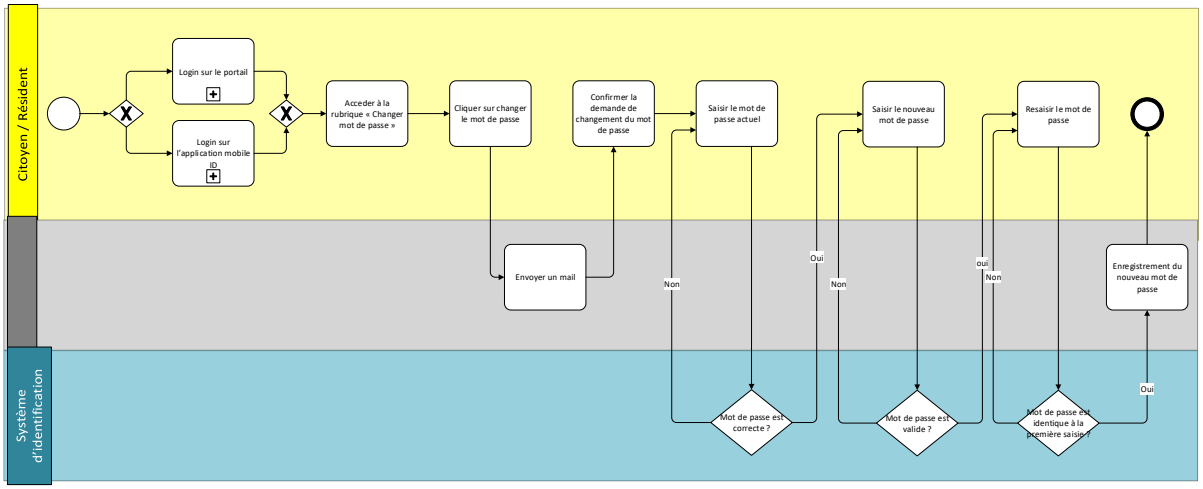


Figure 39 : Processus de la mise à jour du mot de passe

Ci-dessous le tableau détaillant les étapes ci-dessus.

Etape	Responsable/Système	Description
Lancer l'application Mobile	Citoyen/Résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Lancer le Portail	Citoyen/Résident	
Accéder à la rubrique « Changer le mot de passe »	Citoyen/Résident	Le citoyen/résident accède à la rubrique « Changer mot de passe » afin de changer son mot de passe
Cliquer sur changer le mot de passe	Citoyen/Résident	Pour continuer les étapes suivantes, le citoyen/résident devra cliquer sur l'option "Changer le mot de passe"
Envoyer un mail	Système d'identification	Pour des raisons de sécurité, un mail sera adressé au citoyen/résident afin de vérifier son identité.
Confirmer la demande de changement du mot de passe	Citoyen/Résident	Une fois que le citoyen/résident a confirmé son identité, il sera autorisé à modifier son mot de passe
Saisir le mot de passe actuel	Citoyen/Résident	Le citoyen/résident saisit son mot de passe actuel.

Etape	Responsable/Système	Description
Mot de passe correct ?	Système d'identification	Le système d'identification doit vérifier si le mot de passe saisi est correct ou pas
Saisir le nouveau mot de passe	Citoyen/Résident	En cas de validation du mot de passe actuel, il sera en mesure de saisir le nouveau mot de passe.
Mot de passe est valide ?	Système d'identification	Le mot de passe doit être conforme aux critères exigés : • Une taille minimale de 10 caractères. • Contient au moins une lettre en majuscule • Contient au moins une lettre en minuscule • Contient au moins un chiffre. • Contient au moins un caractère spécial (#, @, *, etc.)
Ressaisir le nouveau mot de passe	Citoyen/Résident	Le citoyen/résident doit entrer à nouveau son nouveau mot de passe.
Mot de passe est identique à la première saisie ?	Système d'identification	Si les deux entrées correspondent, alors le mot de passe sera mis à jour.
Enregistrement du nouveau mot de passe	Système d'identification	Si la saisie du nouveau mot de passe est correcte, il sera enregistré dans la base de données.

Tableau 39 : Tableau descriptif du processus de la mise à jour du mot de passe

7.7.2 Mise à jour du PIN

Afin de gérer au mieux son profil et dans un souci d'optimisation des procédures sécuritaires du compte du citoyen/résident dans l'application mobile ou dans le portail fID, le citoyen/résident aura la possibilité de mettre à jour son PIN au besoin.

Ci-dessous le processus qui décrit les étapes à suivre pour mette à jour le PIN sur l'application mobile.

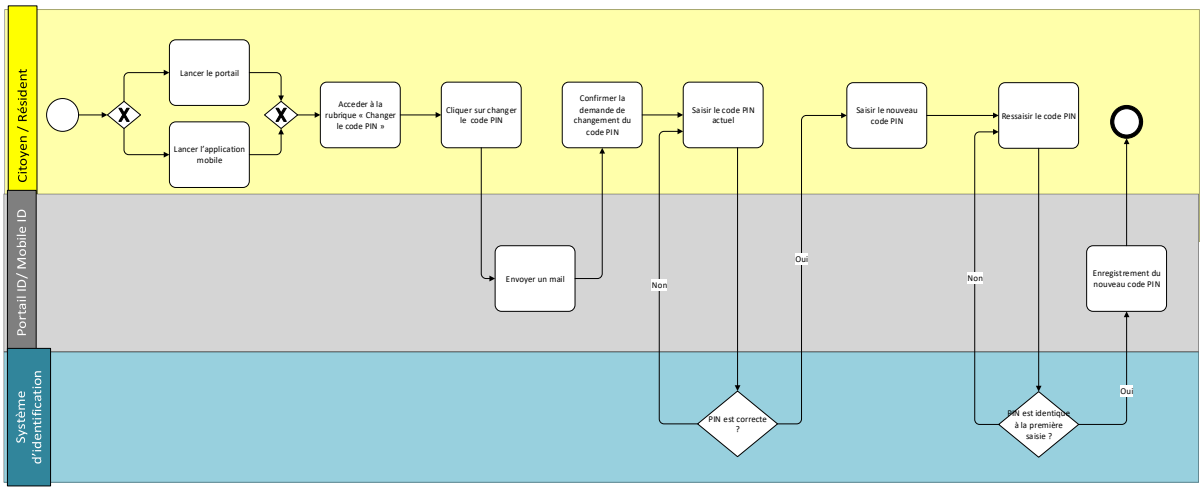


Figure 40 : Processus de la mise à jour du code PIN

Ci-dessous le tableau détaillant les étapes ci-dessus.

Etape	Responsable/Système	Description
Lancer l'application Mobile	Citoyen/Résident	Le citoyen/résident peut se connecter à son compte via le portail fID ou via l'application mobile
Lancer le Portail	Citoyen/Résident	
Accéder à la rubrique « Changer le code PIN »	Citoyen/Résident	Le citoyen/résident accède à la rubrique « Changer le code PIN » afin de changer son PIN.
Cliquer sur changer le code PIN	Citoyen/Résident	Pour continuer les étapes suivantes, le citoyen/résident devra cliquer sur l'option « Changer le code PIN »
Envoyer un mail	Système d'identification	Dans un souci de sécurité, un mail sera adressé au citoyen/résident afin de vérifier son identité.
Confirmer la demande de changement du code PIN	Citoyen/Résident	Une fois que le citoyen/résident a confirmé son identité, il sera autorisé à modifier son mot de passe
Saisir le code PIN actuel	Citoyen/Résident	Le citoyen/résident saisit son code PIN actuel.
PIN correct ?	Système d'identification	Le système d'identification doit vérifier sir le PIN saisi est correct ou pas
Saisir le nouveau code PIN	Citoyen/Résident	En cas de validation du code PIN actuel, il sera en mesure de saisir le nouveau code PIN.
Ressaisir le nouveau code PIN	Citoyen/Résident	Le citoyen/résident doit entrer à nouveau son nouveau PIN.
PIN est identique à la première saisie ?	Système d'identification	Si les deux entrées correspondent, alors le code PIN sera mis à jour.
Enregistrement du nouveau code PIN	Système d'identification	Si la saisie du nouveau code PIN est correcte, il sera enregistré dans la base de données.

Tableau 40 : Tableau descriptif du processus de mise à jour code PIN

7.7.3 Mot de passe oublié

Afin de garantir l'accessibilité à son compte du citoyen/résident dans l'application mobile ou dans le portail fID, le citoyen/résident aura la possibilité de créer un nouveau mot de passe s'il a oublié son mot de passe.

Ci-dessous le processus qui décrit les étapes à suivre pour récupérer le mot de passe sur le portail fID et sur l'application mobile.

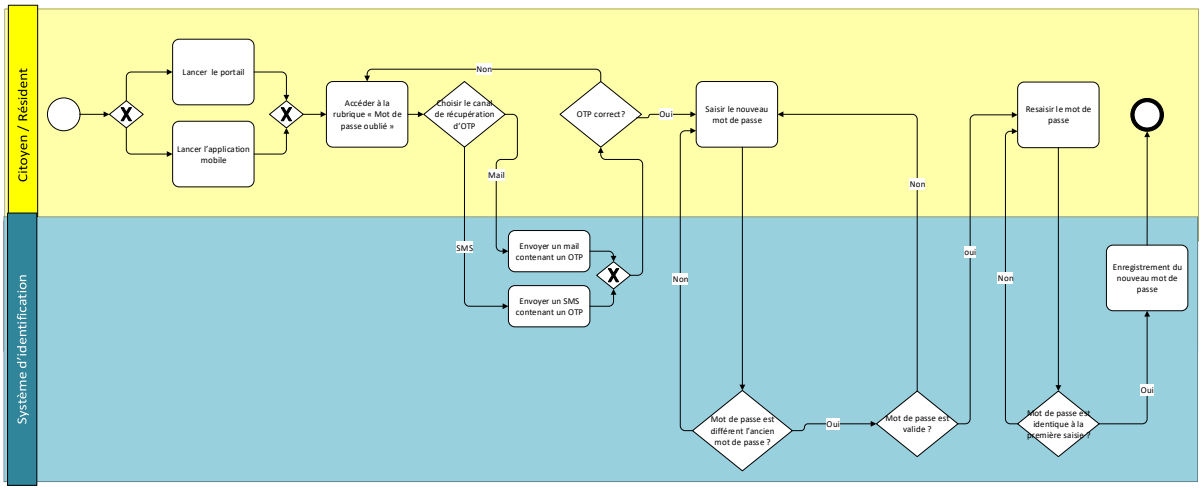


Figure 41 : Processus mot de passe oublié

Ci-dessous le tableau détaillant les étapes ci-dessus.

Etape	Responsable/Système	Description
Lancer l'application Mobile	Citoyen/Résident	Le citoyen/résident accède au portail fID ou à l'application mobile
Lancer le Portail	Citoyen/Résident	
Accéder à la rubrique « Mot de passe oublié »	Citoyen/Résident	Le citoyen/résident accède à la rubrique « Mot de passe oublié » afin de récupérer son mot de passe.
Envoyer un mail contenant un OTP	Système d'identification	Dans un souci de sécurité, un mail sera adressé au citoyen/résident afin de vérifier son identité.
Envoyer un SMS contenant un OTP	Système d'identification	Dans un souci de sécurité, un SMS sera adressé au citoyen/résident afin de vérifier son identité.
OTP correct ?	Système d'identification	Le système d'identification doit vérifier sir l'OTP saisi est correct ou pas
Saisir le nouveau mot de passe	Citoyen/Résident	En cas de validation du code OTP envoyé, il sera en mesure de saisir le nouveau mot de passe.
Nouveau mot de passe est différent de l'ancien mot de passe ?	Système d'identification	Le système vérifie que le nouveau mot de passe saisi est différent de l'ancien enregistré dans la base de données.
Si oui, Vérifier que le mot de passe saisi est valide	Système d'identification	Si le nouveau mot de passe est différent de l'ancien, le système vérifiera si le nouveau mot de passe répond aux exigences suivantes : • Une taille minimale de 10 caractères. • Contient au moins une lettre en majuscule

Etape	Responsable/Système	Description
		• Contient au moins une lettre en minuscule • Contient au moins un chiffre. • Contient au moins un caractère spécial (#, @, *, etc.)
Si le mot de passe est valide, ressaisir le nouveau mot de passe	Citoyen/Résident	Le citoyen/résident doit entrer à nouveau son nouveau mot de passe.
Mot de passe est identique à la première saisie ?	Système d'identification	Si les deux entrées correspondent, alors le mot de passe sera mis à jour.
Enregistrement du nouveau mot de passe	Système d'identification	Si la saisie du nouveau mot de passe est correcte, il sera enregistré dans la base de données.

Tableau 41 : Tableau descriptif du processus mot de passe oublié

7.7.4 PIN oublié

Afin de garantir l'accessibilité à son compte du citoyen/résident dans l'application mobile, le citoyen/résident aura la possibilité de créer un nouveau PIN s'il a oublié son PIN actuel.

Ci-dessous le processus qui décrit les étapes à suivre pour récupérer le PIN sur l'application mobile.

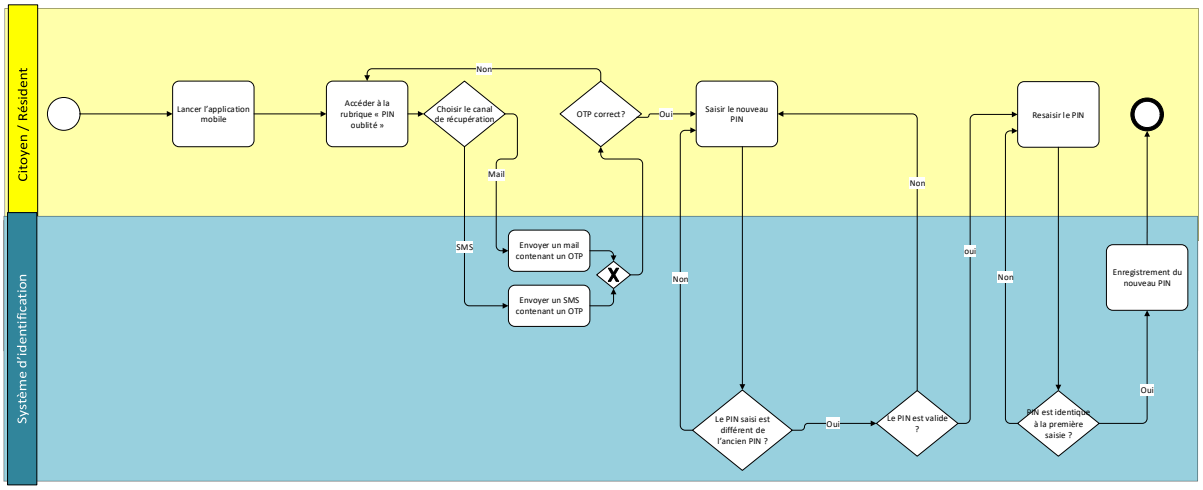


Figure 42 : Processus PIN oublié

Ci-dessous le tableau détaillant les étapes ci-dessus.

Etape	Responsable/Système	Description
Lancer l'application Mobile	Citoyen/Résident	Le citoyen/résident accède à l'application mobile
Accéder à la rubrique « PIN oublié »	Citoyen/Résident	Le citoyen/résident accède à la rubrique « PIN oublié » afin de récupérer son PIN.
Envoyer un mail contenant un OTP	Système d'identification	Dans un souci de sécurité, un mail sera adressé au citoyen/résident afin de vérifier son identité.
Envoyer un SMS contenant un OTP	Système d'identification	Dans un souci de sécurité, un SMS sera adressé au citoyen/résident afin de vérifier son identité.

Etape	Responsable/Système	Description
OTP correct ?	Système d'identification	Le système d'identification doit vérifier sir l'OTP saisi est correct ou pas
Saisir le nouveau PIN	Citoyen/Résident	En cas de validation du code OTP envoyé, il sera en mesure de saisir le nouveau PIN.
Nouveau PIN est différent de l'ancien PIN ?	Système d'identification	Le système vérifie que le nouveau PIN saisi est différent de l'ancien enregistré dans la base de données.
Si oui, Vérifier que le PIN saisi est valide	Système d'identification	Si le nouveau mot de passe est différent de l'ancien, le système vérifie si le nouveau mot de passe répond aux exigences suivantes : • Le PIN est composé de 4 caractères • Tous les caractères sont de type entier
Ressaisir le nouveau PIN	Citoyen/Résident	Le citoyen/résident doit entrer à nouveau son nouveau PIN.
PIN est identique à la première saisie ?	Système d'identification	Si les deux entrées correspondent, alors le PIN sera mis à jour.
Enregistrement du nouveau PIN	Système d'identification	Si la saisie du nouveau PIN est correcte, il sera enregistré dans la base de données.

Tableau 42 : Tableau descriptif du processus PIN oublié

8 Architecture fonctionnelle cible

8. Architecture fonctionnelle cible

8.1 Vues du système d'identification

Un système d'information repose sur quatre vues essentielles : métier, fonctionnelle, applicative, et technique comme le montre la figure ci-dessous, ceci est applicable dans notre contexte au système d'identification.

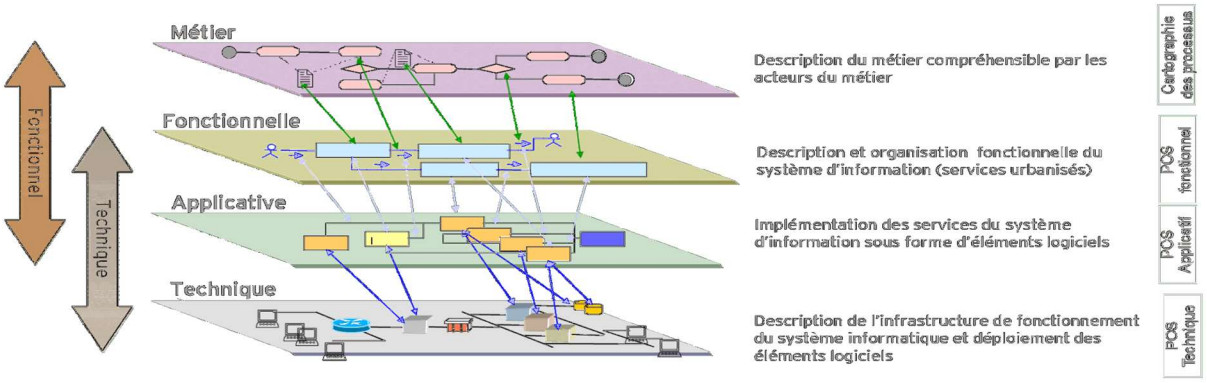


Figure 43 : Vues d'un Système d'information

Notre système d'identification cible est composée d'une :

- **Vue métier:**

Cette vue se concentre sur les processus et activités métiers de l'organisation responsable du système d'identification, sans considérer les détails techniques. Elle illustre comment l'organisation fonctionne en termes de processus, flux d'informations et interactions entre les différentes parties prenantes.

Ci-dessous les processus métiers liés à l'identification et l'authentification qui ont été abordés dans le L9 **« Conception de l'architecture cible du système fID »** et qui ont évolué, été mis à jour et détaillés lors de la rédaction de ce document suite aux travaux survenus lors des derniers mois (Post L9)

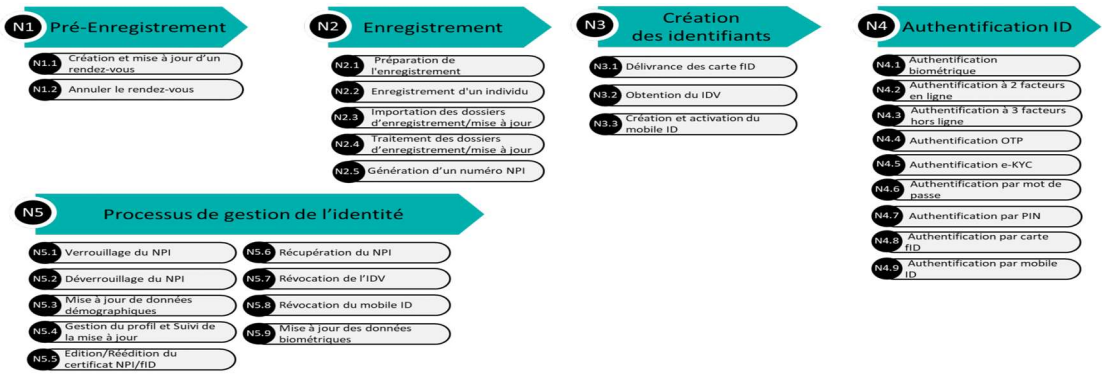


Figure 44 : Cartographie des processus métiers du système d'identification cible

- **Vue fonctionnelle:**

Dans la logique des différentes vues du système d'identification et dans la continuité de ce qui a été réalisé dans le L9 et sur la base des travaux qui ont suivi le L9, l'élaboration de la vue fonctionnelle s'appuie sur la vue métier (processus décrits ci-dessus).

La vue fonctionnelle décrit donc les fonctions nécessaires pour supporter ces processus métiers, elle se situe à un niveau plus détaillé que la vue métier, et elle permet de mettre en évidence le lien entre les processus et les modules à travers l'architecture fonctionnelle proposée (développée à travers le Plan d'occupation des Sols SI décrit dans la section 8.2)

- **Vue applicative:**

Elle représente le paysage des applications et solutions logicielles mises en place pour répondre aux besoins fonctionnels. Elle montre comment ces applications interagissent entre elles et comment elles sont structurées.

- **Vue technique:**

Cette vue concerne l'infrastructure technique nécessaire pour soutenir les applications. Elle se penche sur l'architecture physique du SI, couvrant le matériel, les réseaux, les systèmes d'exploitation et autres composants techniques.

Les vues applicative et technique ne font pas l'objet de ce document vu leurs dépendances par rapport aux choix techniques et à la solution proposée par le fournisseur sélectionné suite au DAO (L16.2 : Acquisition, modernisation et opérationnalisation de l'infrastructure et de la plateforme e-ID pour le site de production (DCN) et le site de secours (DR)).

Cependant, a noter que les points applicatifs et techniques ont été abordés dans le « L9 : Architecture Cible » et dans les travaux sur l'hébergement pour l'architecture technique au sein du Datacenter National.

8.2 Plan d'Occupation des Sols SI (POS SI)

8.2.1 Définition et objectifs

L'architecture fonctionnelle cible est représenté par un POS sous forme de cartographie fonctionnelle du SI qui vise à proposer une grille d'analyse des fonctions offertes par le SI, qu'il organise en catégories fonctionnellement cohérentes.

Le POS permet ainsi d'identifier des redondances fonctionnelles, d'établir une cible fonctionnelle indépendante de l'organisation, de maîtriser le respect de certaines règles d'urbanisation (référentiels, non-duplication…), d'identifier et projeter les rationalisations ou mutualisations possibles, et contribue à la bonne gouvernance du SI.

Concernant la représentation du POS, celui-ci présente généralement seulement trois niveaux de blocs (zone, quartier et ilot) définis comme suit :

- **Zone**

Regroupement de plus haut des fonctions du SI, portant la vision urbanisée recherchée du SI, et justifiée sur la base de principes d'urbanisation. Elles sont divisées en quartiers.

- **Quartier**

Regroupement d'îlots traitant des données de même nature fonctionnelle

- **îlot**

Unité fonctionnelle regroupant les traitements et accès à un ensemble de données fortement cohérentes fonctionnellement.

L'architecture fonctionnelle cible n'est pas figée dans le temps et sera amenée à évoluer, au rythme des évolution fonctionnelles et techniques du métier et du SI associé.

8.2.2 Principe du zonage du POS SI

Dans le découpage en zone POS SI, nous distinguons différents types de zones comme montré dans la figure ci-dessous :

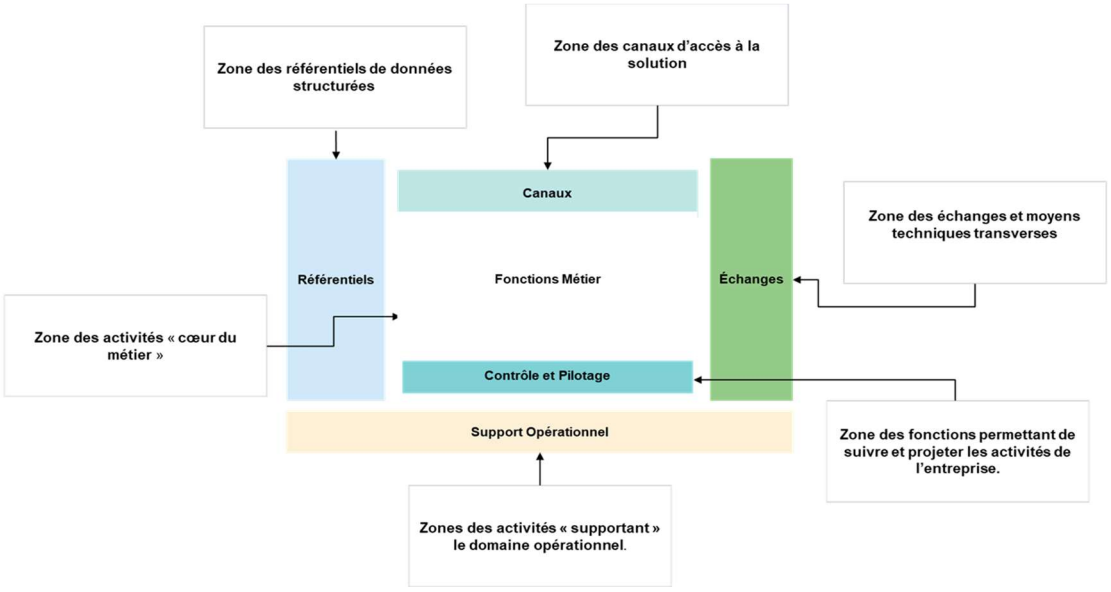


Figure 45 : Principe de zonage du POS SI

Ci-dessous le tableau décrivant chacune de ces zones pour le système d'identification cible :

N°	Zone	Description
Z1	**Référentiels**	Désigne les bases de données que le système d'identification utilise
Z2	**Canaux**	Désigne l'interface externe des services du système d'identification, cette zone regroupe donc les fonctions d'interaction avec les utilisateurs du système, elle regroupe les flux qui émanent ou sont à destination d'acteurs externes : partenaires, autorités, autres organisations, etc. Considérée ainsi comme la « prise » ou le « connecteur » du Système.

Z3	**Echanges**	Désigne les échanges internes ou externe au système d'identification et inter-système d'information avec par exemple les partenaires, les autorités de tutelle, les moyens de paiement, le moteur de workflow etc.
Z4	**Métier**	Désigne le cœur du métier de l'organisation responsable de l'identification (en l'occurrence l'ANIP).
Z5	**Contrôle et pilotage**	Permet de suivre et projeter les activités de l'organisation responsable de l'identification, elle comprend les indicateurs permettant de suivre la stratégie tels que l'audit et monitoring ainsi que le module BI/analytics
Z6	**Support Opérationnel**	Dans cette zone, se retrouvent les activités dites support ou socles de l'organisation : Finance, communication, GED, sécurité et helpdesk IT.

Tableau 43 : Les zones pour le système d'identification cible

Nous avons mis en évidence les relations fonctionnelles qui existent entre les différentes zones du POS SI comme montré dans la figure ci-dessous.

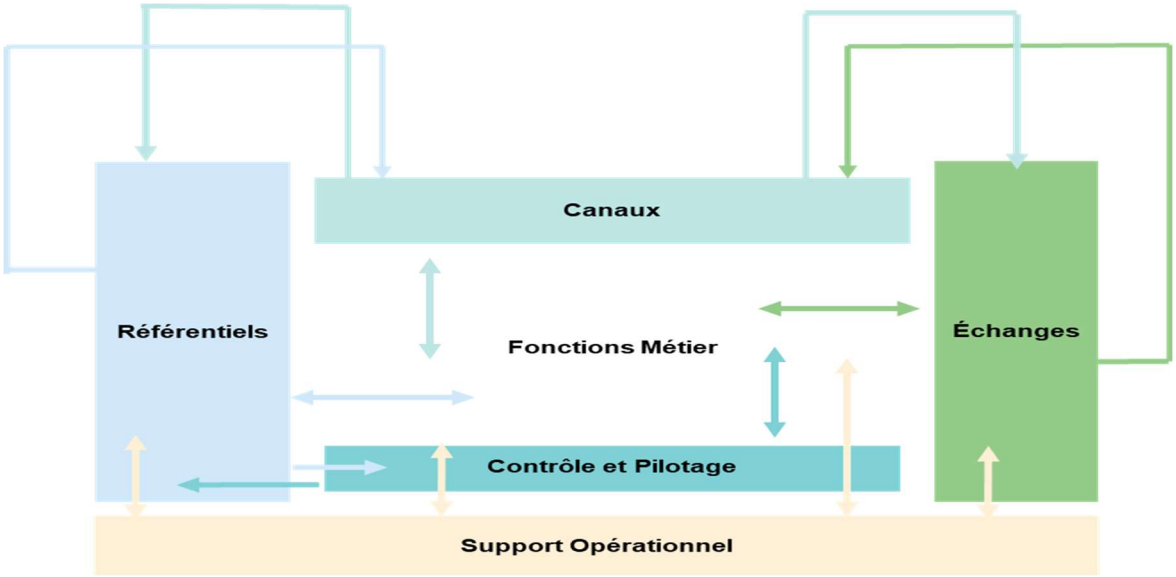


Figure 46 : Liens fonctionnels entre les zones

Les liens fonctionnels entre les différentes zones du système d'identification cible sont cruciaux pour assurer une synergie globale et un fonctionnement intégré**.**

Quelques exemples de relations fonctionnelles entre les différentes zones :

- **Les échanges** tant internes qu'externes, sont intrinsèquement liés aux interfaces des **Canaux** car c'est par **ces canaux** agissent comme des points d'entrée et de sortie des informations et données provenant du système d'identification via la **zone métiers** (ex : Services d'authentification) vers les **plateformes externes via la zone échange** (ex : SIG RSU, SIG Gbessoké…) ou l'inverse.

- **Les données métiers** collectés sont stockées dans les **référentiels** et peuvent être utilisées pour créer des **tableaux de bord et des rapports BI** ainsi que le monitoring et l'audit qui se trouvent dans la **zone contrôle et pilotage**.
- Le **Support Opérationnel** soutient **toutes les zones** en fournissant des services essentiels, tels que la gestion financière, la communication, la sécurité, et l'assistance informatique, contribuant ainsi au bon fonctionnement de l'ensemble du système d'identification.

Ces liens fonctionnels créent une interdépendance nécessaire pour garantir une opération fluide, cohérente et alignée sur les objectifs stratégiques du système d'identification.

8.3 Architecture fonctionnelle cible

La mise en place d'une architecture fonctionnelle cible du système d'identification bien définie permet au projet WURI Bénin de s'assurer qu'elle dispose des structures et des processus appropriés pour répondre à ses objectifs stratégiques et métiers tout en offrant une expérience optimale aux citoyens/résidents et en garantissant la fluidité et l'efficacité de ses opérations.

Sur la base des travaux effectués précédemment sur les processus et applicatifs et sur la base du principe du zonage du POS SI, nous avons élaboré l'architecture fonctionnelle globale cible.

La vision de l'architecture cible proposée consiste à ce que le fID et son écosystème viennent compléter le système RNPP déjà existant, afin de permettre la couverture de l'ensemble de la population (groupes vulnérables, population carcérales, diaspora etc.) et assurer la sécurité en matière de protection des données à caractère personnel et de la vie privée.

La vision architecturale doit donc faire un focus particulier sur le fait que le système cible devra être complet en termes de besoin métier. En effet, la solution fID à mettre en place devra capitaliser sur l'écosystème d'identification biométrique au Bénin tout en permettant que l'écosystème d'identification soit évolutif et durable.

Ainsi, en prenant en compte les besoins de l'Etat Béninois et les principes de la Banque Mondiale, la vision de l'architecture de la solution fID doit être en ligne avec la vision stratégique suivante : « Mettre en œuvre un système d'identification complémentaire au système actuel, inclusif, durable, évolutif et interopérable permettant la rationalisation et l'optimisation de la prestation des services publics et privés aux béninois et aux résidents sur le sol béninois ».

L'urbanisation du système d'identification cible doit se faire selon une logique modulaire. Les différents domaines fonctionnels doivent être conçus tels que des « produits » auxquels viennent se rattacher les composants de la plateforme. Tous les composants du système d'identification en cible doivent donc être modulaires avec des fonctionnalités exposées via des API, et toutes modifications d'un composant doit se faire sans affecter les autres modules.

L'architecture fonctionnelle proposée se compose de six zones distinctes, et pour chacune de ces « **Zones »,** nous avons défini un domaine fonctionnel spécifique, connu sous le nom **de « Quartier »**. Chacun de ces

domaines fonctionnels est subdivisé en sous-domaines fonctionnels connu sous le **nom « d'Ilot »**, comme précisé dans le document intitulé "L9 - Conception de l'architecture cible du système fID".

- **Zone métier**

Dans la zone métier, nous identifions trois domaines fonctionnels essentiels : le domaine de l'enregistrement des citoyens/résidents, le domaine de gestion de l'identité et le domaine de gestion des partenaires. Ces trois domaines représentent le cœur des opérations du système d'identification cible. Ils seront supervisés par des fonctionnalités d'audit et de reporting, tout en bénéficiant du support de fonctions telles que la gestion financière, la communication, la gestion électronique de documents (GED) et le support technique tout en garantissant la sécurité du système en raison de la nature confidentielle et critique des données manipulées.

- **Zone échanges**

Le système sera capable d'interagir avec d'autres systèmes externes, tels que le SIG (système Intégré de Gestion) Gbessoké et RSU ainsi le Gateway (ex : passerelle de paiement), à travers XROAD.

- Le SIG est un ensemble organisé de ressources qui facilite la collecte, le traitement, la gestion et la diffusion des données essentielles aux opérations du programme de protection sociale, à la responsabilisation et à la prise de décision. Le SIG assure la gestion précise et opportune de données volumineuses, souvent sur plusieurs sites et à plusieurs niveaux de mise en œuvre du programme :
  - Le SIG RSU et Gbessoké, devront être interopérables avec le système d'identification cible qui permettra de faire le lien entre les différentes information grâce au NPI.
  - Le RSU est un système d'information qui appuie les processus d'inscription et de décision quant à l'éligibilité, à travers la collecte et la mise à jour des informations sur les bénéficiaires potentiels des programmes de protection sociale.
  - Quant à Gbessoké, c'est un système qui sera mis en place en vue d'améliorer les capacités de pilotage et de gouvernance des projets et programmes sociaux du ministère des Affaires Sociales et de la Microfinance (MASM).
- L'accès aux services publics/privés se fera via une authentification qui devra passer via **XRoad.** Les entités privées devront mettre en place des serveurs de sécurité qui seront les seules habilités à se connecter à la base de données PostgreSQL et ainsi avoir accès aux données d'identification
- La passerelle de paiement:
  Cette passerelle doit avoir au minima les fonctionnalités suivantes :
  - Plusieurs options de paiement (exemple : les terminaux de paiement électronique, les cartes de crédit et de débit, les interfaces de paiement des banques, les paiements mobiles, etc.)
  - Gestion des opérations de remboursement
  - Lien de paiement direct
  - Cryptages des données de paiement

Le système de paiements liés au fID et NPI devra s'intégrer à l'existant et devra effectivement s'arrimer avec la PNPE de l'Etat, qui est un hub pour les solutions numériques de paiement.

La figure ci-dessous illustre et explique le positionnement des systèmes externes ainsi que les interactions possibles entre eux.

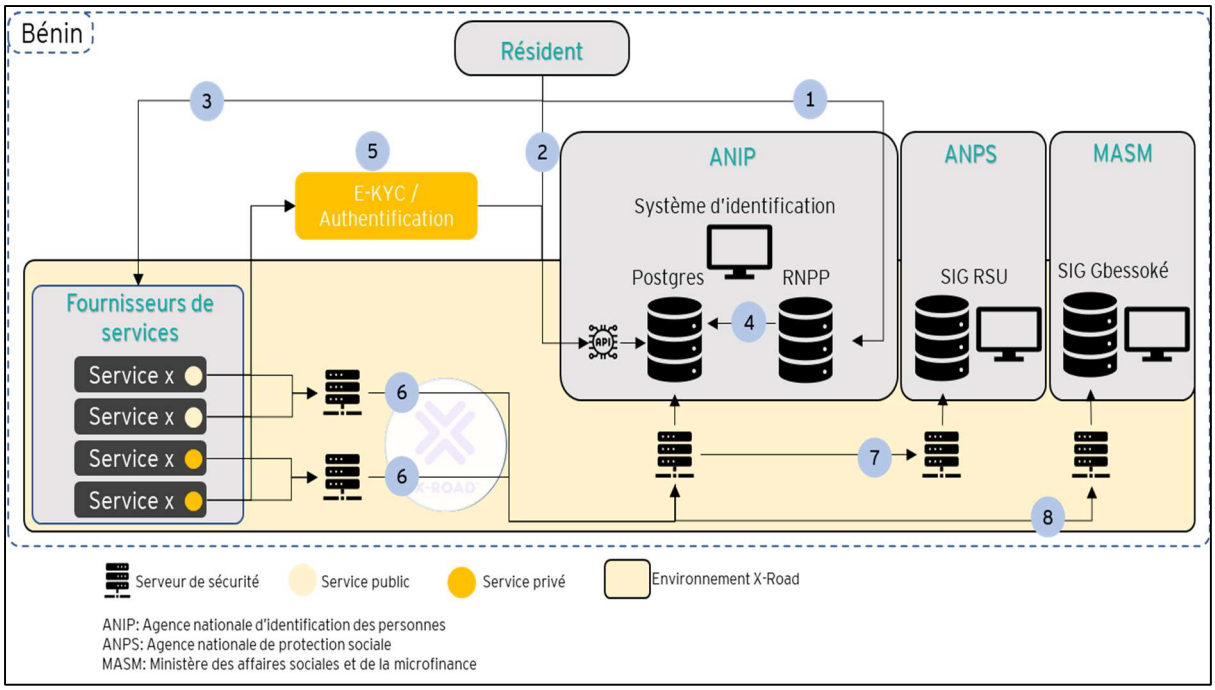


Figure 47 : Modèle d'interaction du système d'identification avec l'environnement national

Il faut noter que cette modélisation ne prend en considération que les interactions possibles dans le contexte du projet en cours. Plusieurs autres systèmes sont déjà sur X-Road et peuvent interagir avec le système d'identification, le modèle présenté pourra évoluer en fonction des nouveaux services.

- **Zone référentiel**

Dans la zone référentielle, le système d'identification cible utilisera :

o Des données minimales stockées dans la base de données PostgreSQL pour identifier et authentifier les individus comme montré dans la figure ci-dessous

Les données minimales requises comprennent :

- Des informations démographiques tels que le nom, le prénom, le genre et le NPI (Numéro de Personne d'Identification)
- Des données biométriques : les modèles des 10 empreintes digitales une fois capturées, ainsi qu'un modèle de portrait.
- Des données de contact, tel que le numéro de téléphone à des fins d'authentification,
- Des données liées aux transactions, tels que la date du recensement et le type de demande

Cette base de données minimale sera accessible via une API externe et sera synchronisée en temps réel avec la base de données RNPP.

Cette synchronisation sera effectuée dans un seul sens : de la base de données RNPP vers la base de données PostgreSQL afin de limiter tout risque d'accès ou de modification sur la base de données RNPP vu sa criticité.

La figure ci-dessous illustre la relation entre les deux bases de données

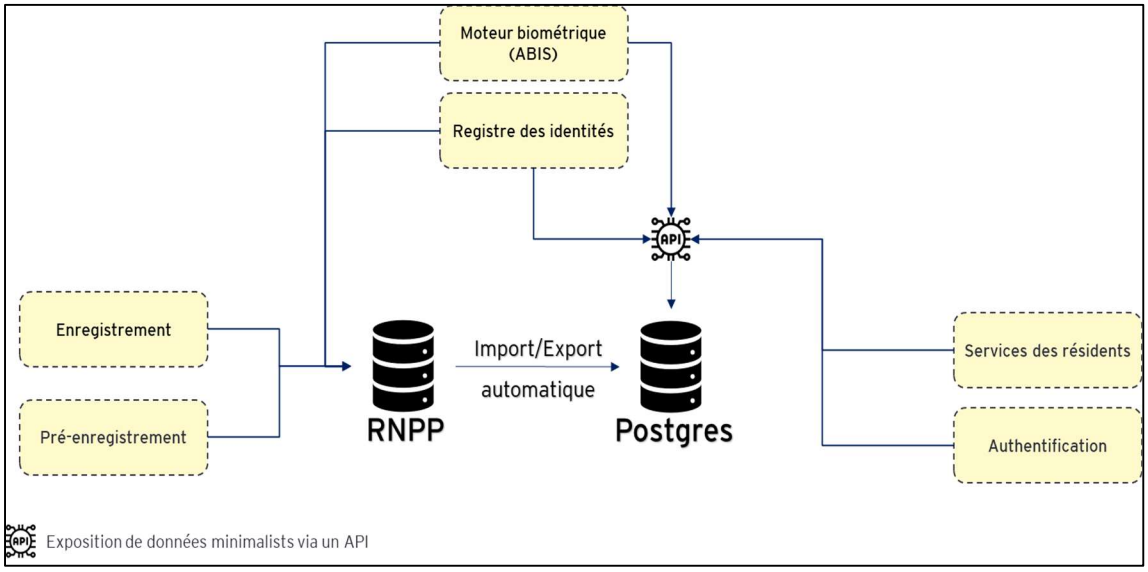


Figure 48 : Relations entre la base RNPP et PostgreSQL

- Le registre d'état civil : Ce registre est utilisé pour enregistrer et documenter les événements vitaux de la vie d'une personne, tels que les naissances, les mariages, les divorces et les décès, IL joue un rôle crucial dans la reconnaissance juridique et sociale d'une personne et il est inclus dans la base de données Postgres.

- **Zone canaux**

Concernant la zone canaux, elle sera détaillée dans la section 8.3.2.

- **Zone contrôle et pilotage**

Pour la zone contrôle et pilotage elle est compose de deux domaines fonctionnes contrôle et audit internes, et reporting, et regroupe des fonctions permettant de suivre et projeter les activités de l'organisation qui sont les outils BI, l'audit et le monitoring.

- **Zone support opérationnel**

Cette zone regroupe les fonctions support. Elle se compose des domaines fonctionnels suivants :

- Finance : composé de sous domaine facturation
- Communication : fonctions supportant les communications internes et externes
- GED
- Sécurité (chiffrement des données et gestion des fraudes)
- Helpdesk IT (support IT, gestion des incidents, gestion des accès)

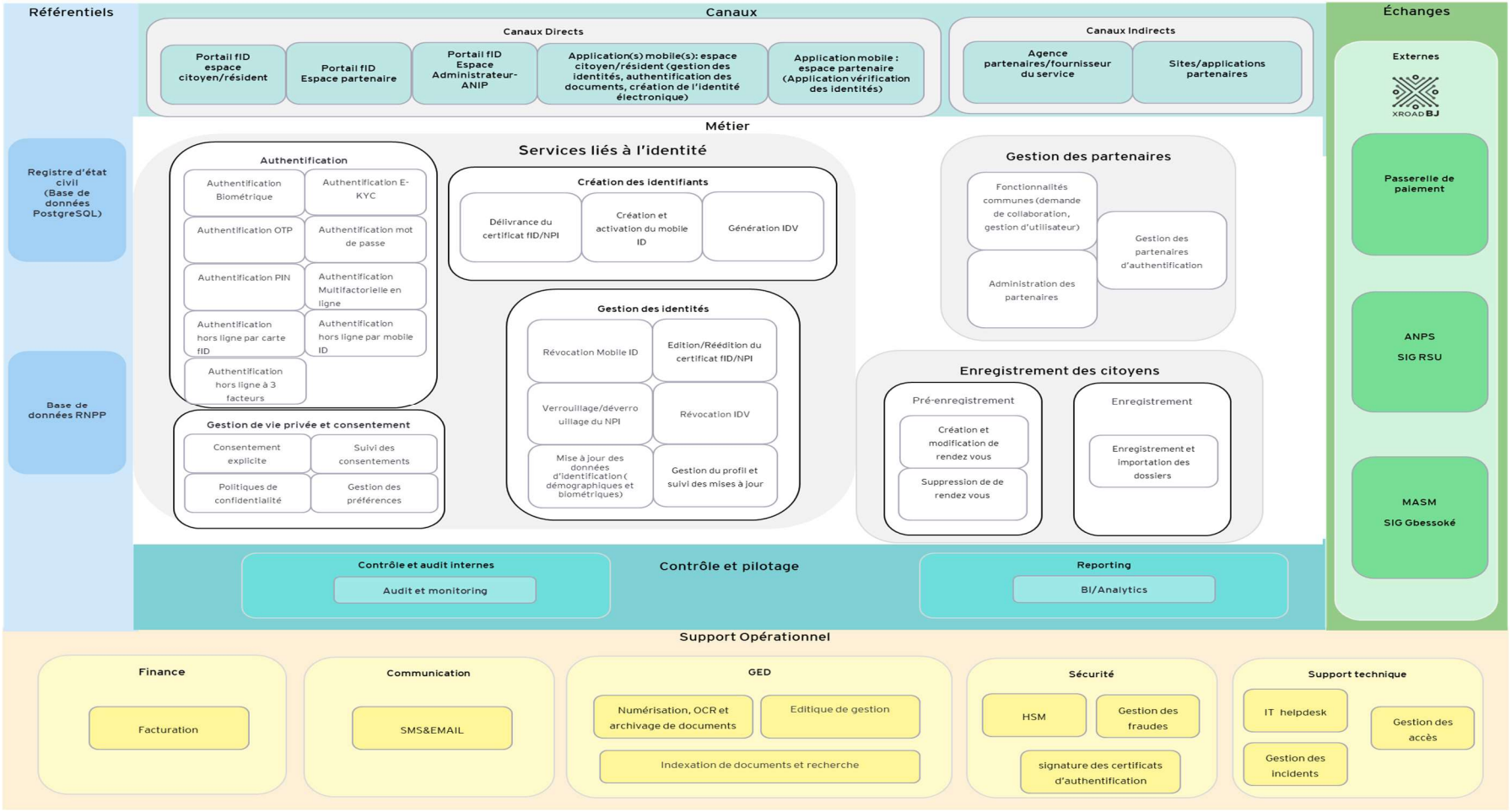


Figure 49 : Architecture fonctionnelle cible globale

8.3.2 Architecture fonctionnelle cible : Zoom sur les canaux

La zone canaux se compose de deux volets :

- **Les canaux directs,** qui vont typiquement regrouper les applications en interactions directe avec le client : portail client, applications mobiles, communication sur les réseaux sociaux, etc
- **Les canaux indirects,** qui vont typiquement regrouper les APIs exposées à des tiers, les applications mises à dispositions de partenaires, etc.

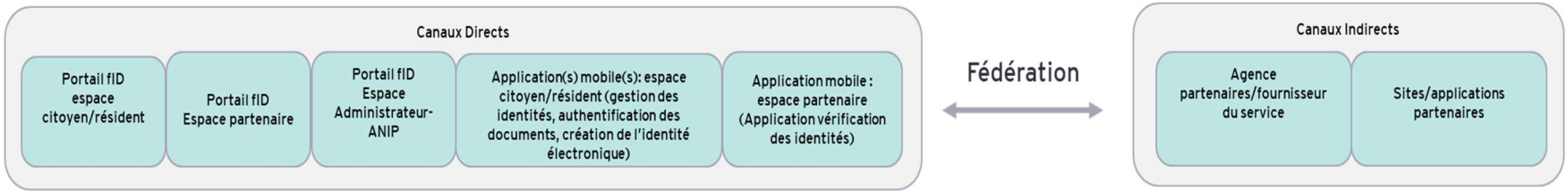


Figure 50 : Lien entre les canaux

La fédération entre ces deux canaux permet au citoyen/résident :

- Lorsqu'il accède à un site partenaire, d'être redirigé vers le portail fID où il s'authentifie. Une fois l'authentification réussie, un jeton d'authentification est généré et renvoyé au site partenaire, confirmant l'identité de l'utilisateur. Le site partenaire peut ensuite accorder l'accès à ses services. Ceci permet aux sites des partenaires de faire confiance au système d'identification des citoyens/résidents pour authentifier les utilisateurs.

- Lorsqu'il accède à son compte sur le portail fID ou l'application mobile, une fois authentifié avec succès, d'avoir accès au site du partenaire sans avoir besoin de se réauthentifier.

8.3.3 Architecture fonctionnelle cible : zoom sur les fonctionnalités

Dans cette partie, nous nous focaliserons sur les blocs liés à l'identification et l'authentification qui font l'objet du présent document et sur leurs fonctionnalités respectives en se conformant aux détails des processus métiers développés dans la première partie du document.

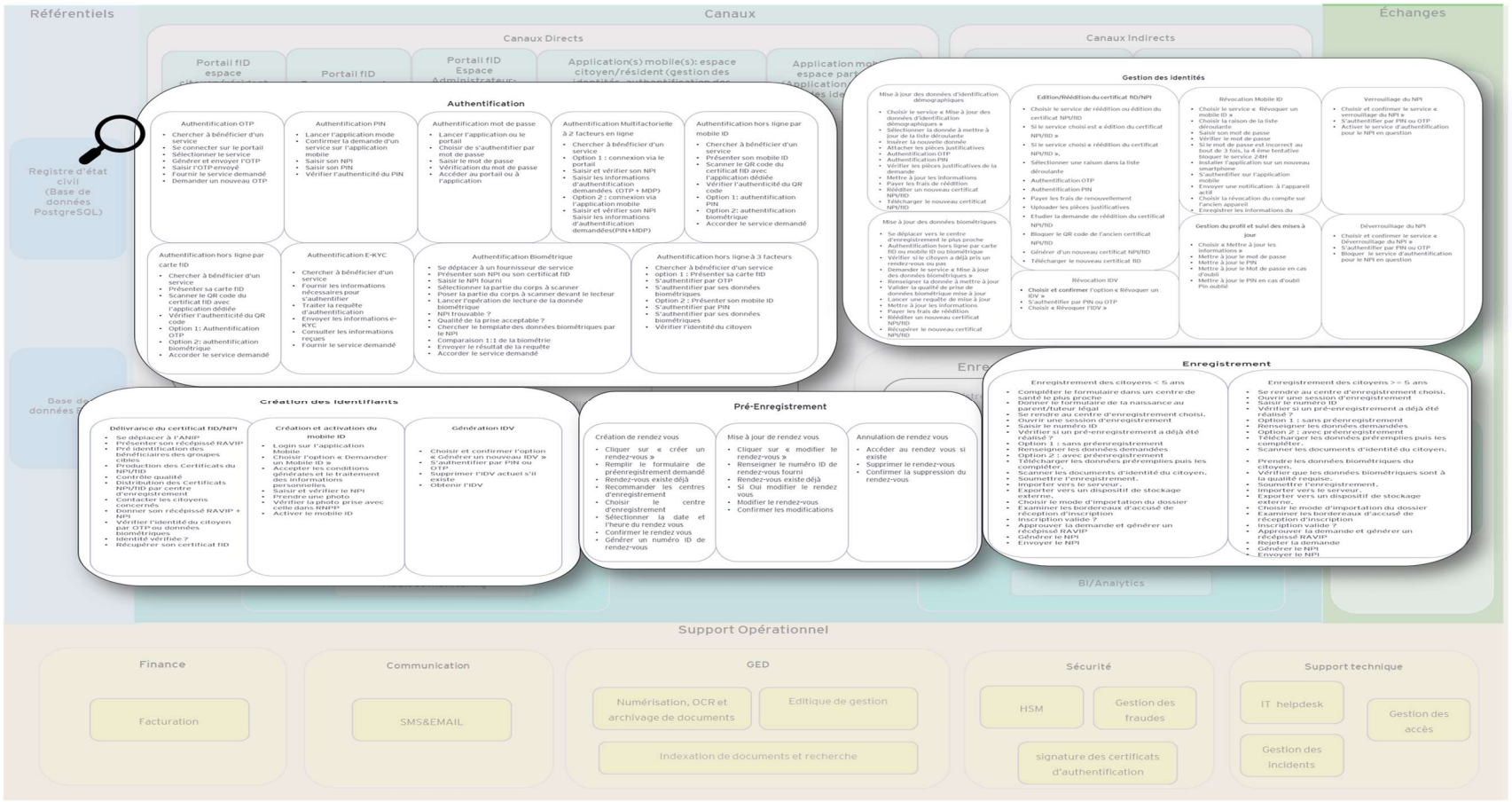


Figure 51 Architecture fonctionnelle cible : zoom sur les fonctionnalités

Ci-dessous la liste des fonctionnalités par quartier et par Ilot présentés dans la figure précédente :

Création de rendez-vous

- Cliquer sur « créer un rendez-vous »
- Remplir le formulaire de préenregistrement demandé
- Rendez-vous existe déjà
- Recommander les centres d'enregistrement
- Choisir le centre d'enregistrement
- Sélectionner la date et l'heure du rendez vous
- Confirmer le rendez vous
- Générer un numéro ID de rendez-vous

Mise à jour de rendez-vous

- Cliquer sur « modifier le rendez-vous »
- Renseigner le numéro ID de rendez-vous fourni
- Rendez-vous existe déjà
- Si Oui modifier le rendez vous
- Modifier le rendez-vous
- Confirmer les modifications

Annulation de rendez-vous

- Accéder au rendez-vous si existe
- Supprimer le rendez-vous
- Confirmer la suppression du rendez-vous

Enregistrement des citoyens < 5 ans

- Compléter le formulaire dans un centre de santé le plus proche
- Donner le formulaire de la naissance au parent/tuteur légal
- Se rendre au centre d'enregistrement choisi.
- Ouvrir une session d'enregistrement
- Saisir le numéro ID
- Vérifier si un pré-enregistrement a déjà été réalisé ?

- Option 1 : sans préenregistrement
- Renseigner les données demandées
- Option 2 : avec préenregistrement
- Télécharger les données préremplies puis les compléter.
- Scanner les documents d'identité du citoyen.
- Soumettre l'enregistrement.
- Importer vers le serveur.
- Exporter vers un dispositif de stockage externe.
- Choisir le mode d'importation du dossier
- Examiner les bordereaux d'accusé de réception d'inscription
- Inscription valide ?
- Approuver la demande et générer un récépissé RAVIP
- Générer le NPI
- Envoyer le NPI

Enregistrement des citoyens >= 5 ans

- Se rendre au centre d'enregistrement choisi.
- Ouvrir une session d'enregistrement
- Saisir le numéro ID
- Vérifier si un pré-enregistrement a déjà été réalisé ?
- Option 1 : sans préenregistrement
- Renseigner les données demandées
- Option 2 : avec préenregistrement
- Télécharger les données préremplies puis les compléter.
- Scanner les documents d'identité du citoyen.
- Prendre les données biométriques du citoyen.
- Vérifier que les données biométriques sont à la qualité requise.
- Soumettre l'enregistrement.
- Importer vers le serveur.
- Exporter vers un dispositif de stockage externe.

- Choisir le mode d'importation du dossier
- Examiner les bordereaux d'accusé de réception d'inscription
- Inscription valide ?
- Approuver la demande et générer un récépissé RAVIP
- Rejeter la demande
- Générer le NPI
- Envoyer le NPI

Authentification par mot de passe

- Lancer l'application ou le portail
- Choisir de s'authentifier par mot de passe
- Saisir le mot de passe
- Vérification du mot de passe
- Accéder au portail ou à l'application

Authentification PIN

- Lancer l'application mode
- Confirmer la demande d'un service sur l'application mobile
- Saisir son NPI
- Saisir son PIN
- Vérifier l'authenticité du PIN

Authentification OTP

- Chercher à bénéficier d'un service
- Se connecter sur le portail fID
- Sélectionner le service
- Générer et envoyer l'OTP
- Saisir l'OTP envoyé
- Fournir le service demandé
- Demander un nouvel OTP

Authentification Multifactorielle à 2 facteurs en ligne

- Chercher à bénéficier d'un service
- Option 1 : connexion via le portail
- Saisir et vérifier son NPI
- Saisir les informations d'authentification demandées (OTP + MDP)
- Option 2 : connexion via l'application mobile
- Saisir et vérifier son NPI Saisir les informations d'authentification demandées (PIN+MDP)

Authentification E-KYC

- Chercher à bénéficier d'un service
- Fournir les informations nécessaires pour s'authentifier
- Traiter la requête d'authentification
- Envoyer les informations e-KYC
- Consulter les informations reçues
- Fournir le service demandé

Authentification hors ligne par mobile ID

- Chercher à bénéficier d'un service
- Présenter son mobile ID
- Scanner le QR code du certificat fID avec l'application dédiée
- Vérifier l'authenticité du QR code
- Option 1 : authentification PIN
- Option 2 : authentification biométrique
- Accorder le service demandé

Authentification hors ligne par carte fID

- Chercher à bénéficier d'un service
- Présenter sa carte fID
- Scanner le QR code du certificat fID avec l'application dédiée
- Vérifier l'authenticité du QR code
- Option 1 : Authentification OTP
- Option 2 : authentification biométrique
- Accorder le service demandé

Authentification Biométrique

- Se déplacer à un fournisseur de service
- Présenter son NPI ou son certificat fID
- Saisir le NPI fourni
- Sélectionner la partie du corps à scanner
- Poser la partie du corps à scanner devant le lecteur
- Lancer l'opération de lecture de la donnée biométrique
- NPI trouvable ?
- Qualité de la prise acceptable ?
- Chercher le template des données biométriques par le NPI
- Comparaison 1:1 de la biométrie
- Envoyer le résultat de la requête
- Accorder le service demandé

Authentification hors ligne à 3 facteurs

- Chercher à bénéficier d'un service
- option 1 : Présenter sa carte fID
- S'authentifier par OTP
- S'authentifier par ses données biométriques
- Option 2 : Présenter son mobile ID
- S'authentifier par PIN
- S'authentifier par ses données biométriques
- Vérifier l'identité du citoyen

Délivrance du certificat fID/NPI

- Se déplacer à l'ANIP
- Présenter son récépissé RAVIP
- Pré identification des bénéficiaires des groupes cibles
- Production des Certificats du NPI/fID
- Contrôle qualité
- Distribution des Certificats NPI/fID par centre d'enregistrement
- Contacter les citoyens concernés

- Donner son récépissé RAVIP + NPI
- Vérifier l'identité du citoyen par OTP ou données biométriques
- Identité vérifiée ?
- Récupérer son certificat fID

Obtention IDV

- Choisir et confirmer l'option « Générer un nouveau IDV »
- S'authentifier par PIN ou OTP
- Supprimer l'IDV actuel s'il existe
- Obtenir l'IDV

Création et activation du mobile ID

- Login sur l'application Mobile
- Choisir l'option « Demander un Mobile ID »
- Accepter les conditions générales et le traitement des informations personnelles
- Saisir et vérifier le NPI
- Prendre une photo
- Vérifier la photo prise avec celle dans RNPP
- Activer le mobile ID

Révocation IDV

- Choisir et confirmer l'option « Révoquer un IDV »
- S'authentifier par PIN ou OTP
- Choisir « Révoquer l'IDV »

Verrouillage du NPI

- Choisir et confirmer le service « Verrouillage du NPI »
- S'authentifier par PIN ou OTP
- Activer le service d'authentification pour le NPI en question

Déverrouillage du NPI

- Choisir et confirmer le service « Déverrouillage du NPI »
- S'authentifier par PIN ou OTP

- Bloquer le service d'authentification pour le NPI en question

Révocation mobile ID

- Choisir le service « Révoquer un mobile ID »
- Choisir la raison de la liste déroulante
- Saisir son mot de passe
- Vérifier le mot de passe
- Si le mot de passe est incorrect au bout de 3 fois, la 4 ème tentative bloquer le service 24H
- Installer l'application sur un nouveau smartphone
- S'authentifier sur l'application mobile
- Envoyer une notification à l'appareil actif
- Choisir la révocation du compte sur l'ancien appareil
- Enregistrer les informations du nouvel appareil
- Révoquer Mobile ID

Mise à jour des données d'identification démographiques

- Choisir le service « Mise à jour des données d'identification démographiques »
- Sélectionner la donnée à mettre à jour de la liste déroulante
- Insérer la nouvelle donnée
- Attacher les pièces justificatives
- Authentification OTP
- Authentification PIN
- Vérifier les pièces justificatives de la demande
- Mettre à jour les informations
- Payer les frais de réédition
- Rééditer un nouveau certificat NPI/fID
- Télécharger le nouveau certificat NPI/fID

Mise à jour des données biométriques

- Se déplacer vers le centre d'enregistrement le plus proche

- Option 1 : Authentification hors ligne par carte fID
- Option 2 : Authentification hors ligne par mobile ID
- Option 3 : Authentification biométrique
- Vérifier si le citoyen a déjà pris un rendez-vous ou pas
- Demander le service « Mise à jour des données biométriques »
- Renseigner la donnée à mettre à jour
- Valider la qualité de prise de données biométrique mise à jour
- Lancer une requête de mise à jour
- Mettre à jour les informations
- Payer les frais de réédition
- Rééditer un nouveau certificat NPI/fID
- Récupérer le nouveau certificat NPI/fID

Edition/Réédition du certificat NPI/fID

- Choisir le service réédition du certificat NPI/fID
- Sélectionner une raison dans la liste déroulante
- S'authentifier par PIN ou OTP
- Payer les frais de renouvellement
- Uploader les pièces justificatives
- Bloquer le QR code de l'ancien certificat NPI/fID après étude et confirmation par l'ANIP
- Générer d'un nouveau certificat NPI/fID
- Télécharger le nouveau certificat fID

Gestion du profil et suivi des mises à jour

- Choisir « Mettre à jour les informations »
- Modifier le mot de passe
- Modifier le PIN
- Enregistrer les modifications
- Choisir « Consulter l'historique des transactions réalisées l'ID »

9 Recommandations pour améliorer l'expérience utilisateur

9. Recommandations pour améliorer l'expérience utilisateur

Dans ce chapitre, nous proposons de partager des pistes de réflexions sur des optimisations futures pour le système d'identification du citoyen/résident. Ces recommandations gravitent autour des notions suivantes :

- La facilitation du quotidien des citoyens/résidents
- La simplification des démarches administratives
- Plus de fluidité dans l'expérience utilisateur
- L'amélioration dans l'accès à l'information et aux services
- Une meilleure sécurité pour les espaces numériques

Creuser de nouvelles pistes pour le développement des services liés à l'identification numérique

Le système d'identification au Bénin tout à fait le potentiel d'évoluer vers un service d'identification universel qui offrirait un ensemble innombrable d'avantages et de services.

En effet, il est possible par exemple d'associer à l'identifiant citoyen/résident un portefeuille numérique complet. Véritable coffre-fort numérique, c'est une sorte de « wallet électronique » hébergé sur le smartphone ou n'importe quel autre terminal personnel, qui contient tous les documents personnels importants ou critiques, comme un certificat médical, un diplôme, un permis de conduire, carte grise de véhicule, etc.

L'objectif étant de faciliter le quotidien de la population, et de permettre aux citoyens/résidents de disposer, en toute circonstance, de ses documents en version numérique avec la valeur légale que les originaux.

Le portefeuille européen permet à l'utilisateur de partager les informations d'identification vérifiables uniquement avec les attributs minimalistes nécessaires au service du portefeuille avec le fournisseur de services. Cela peut fonctionner en mode en ligne et hors ligne.

Un exemple d'utilisation typique serait pendant un contrôle routier où l'automobiliste n'aura qu'à fournir son ID accompagné d'autres informations d'identification vérifiables comme le nom et le prénom pour que l'agent puisse vérifier l'identité de la personne et du véhicule, la même logique pourra être appliquée lors des voyages dans les aéroports, la création de comptes bancaires, l'inscription universitaire, le logement etc.

Un concept similaire sera d'ailleurs généralisé en Europe d'ici 2024, le portefeuille d'identité numérique européen, dévoilé au public en 2021, est un dispositif électronique très sécurisé qui réunit en un seul endroit tous les documents dont les européens pourrait avoir besoin pour voyager en Europe de manière très simplifiée et rapide.