



L'Identification pour le développement (ID4D) : Diagnostic des systèmes d'identification en Tunisie

© 2019 Banque internationale pour la reconstruction et le développement / Banque mondiale 1818 H Street NW

Washington D.C., 20433

Téléphone : 202-473-1000

Site Internet : www.worldbank.org

Cet ouvrage, initialement publié en anglais sous le titre *L'Identification pour le développement (ID4D) : Diagnostic des systèmes d'identification en Tunisie*, a été établi par les services de la Banque mondiale avec la contribution de collaborateurs extérieurs. Les observations, interprétations et opinions qui y sont exprimées ne reflètent pas nécessairement les vues de la Banque mondiale, de son Conseil des Administrateurs ou des pays que ceux-ci représentent.

La Banque mondiale ne garantit pas l'exactitude des données contenues dans cet ouvrage. Les frontières, les couleurs, les dénominations et toute autre information figurant sur les cartes du présent ouvrage n'impliquent de la part de la Banque mondiale aucun jugement quant au statut juridique d'un territoire quelconque et ne signifient nullement que l'institution reconnaît ou accepte ces frontières.

Droits et licences

Le contenu de cet ouvrage fait l'objet d'un dépôt légal. La Banque mondiale encourageant la diffusion de ses travaux, cet ouvrage peut être reproduit, en tout ou en partie, à des fins non commerciales à condition qu'une attribution complète à l'ouvrage soit fournie.

Pour tout autre renseignement sur les droits et licences, y compris les droits dérivés, envoyez votre demande, par courrier, à l'adresse suivante : World Bank Publications, The World Bank Group, 1818 H Street NW, Washington, DC 20433 (États-Unis d'Amérique). Télécopie : 202-522-2625. Courriel : pubrights@worldbank.org.

Table des matières

À Propos de L'initiative ID4D	iii
Remerciements	iv
Les abréviations	v
Résumé Exécutif	vii
PARTIE 1. Introduction	1
1. Motivation de la présente étude	1
2. Identification pour le développement	3
PARTIE 2. L'identification en Tunisie : Points forts et Lacunes	7
1. Aperçu de l'écosystème d'identité tunisien	7
2. Systèmes d'identification de base.....	10
Le Registre d'Etat Civil (REC)	10
Carte d'identité nationale (CIN)	16
Projets de « l'identifiant unique de citoyen (IUC) »	20
3. Systèmes d'identification fonctionnels.....	28
Protection sociale	28
Le secteur de la santé	36
Éducation	37
Les taxes.....	37
4. Cadre juridique	38
Projet de loi organique sur la protection des données à caractère personnel (LPDP)	38
Code numérique.....	40
PARTIE 3. Construire un écosystème d'identité numérique pour la Tunisie : Opportunités, défis et recommandations	42
1. Points forts et opportunités.....	42
2. Principales faiblesses et risques.....	46
3. Recommandations.....	50

Tableaux

Tableau 1 . Vue d'ensemble des principaux systèmes d'identification et registres.....	8
Tableau 2 . Autres acteurs gouvernementaux importants dans l'écosystème d'identité.....	9
Tableau 3 . Couverture de l'état civil.....	11
Tableau 4 . Attributs stockés dans la base de données d'enregistrement des naissances Madania	12
Tableau 5 . Stockage et transfert de données de Madania	13
Tableau 6 . Certificats et extraits de naissance	14
Tableau 7 . Couverture de la CIN.....	16
Tableau 8 . Administration de CIN.....	16
Tableau 9 . Carte et numéro CIN.....	17
Tableau 10 . Données et documents requis pour l'obtention de la CIN.....	18
Tableau 11 . Stockage et transfert de données pour la CIN	18
Tableau 12 . Données à stocker dans le RIUC (en arabe et en français).....	24
Tableau 13 . Liste des premiers services développés pour le RIUC.....	26
Tableau 14 . Résumé de l'IS.....	30
Tableau 15 . Récapitulatif de l'identification pour les principaux systèmes de protection sociale	31
Tableau 16 . Problèmes liés à la qualité et à la précision des données dans les systèmes clés.....	48
Tableau 17 . Avantages potentiels d'un registre d'identités unique pour la prestation de services	51
Tableau 18 . Exemples de technologies et de contrôles opérationnels renforçant la confidentialité.....	56

Graphiques

Schéma 1 . Système d'identification unique projeté.....	vi
Schéma 2 . L'identité en tant que plateforme de développement.....	4
Schéma 3 . Principes de l'identification pour le développement durable	6
Schéma 4 . Systèmes d'identification de base en Tunisie.....	10
Schéma 5 . Structure du numéro de référence du REC (Madania)	14
Schéma 6 . Demande de services en ligne projetée pour des certificats de naissance demande en ligne	15
Schéma 7 . Nouvelle CIN (après 1993)	17
Schéma 8 . Ancienne CNI remise au premier président tunisien, Habib Bourguiba	17
Schéma 9 . Système d'IUC projeté.....	20
Schéma 10 . Structure prévue du numéro IUC	25
Schéma 11 . Génération de l'IS.....	29
Schéma 12 . Processus de vérification des bénéficiaires de la CNAM.....	34

À Propos de L'initiative ID4D

L'initiative Identification pour le développement (ID4D) du Groupe de la Banque mondiale mobilise les connaissances et savoir-faire de différents secteurs partout dans le monde, dans le but d'aider les pays à réaliser le potentiel transformationnel qu'offrent les systèmes d'identification numérique, et ainsi atteindre les Objectifs de développement durable. Mise en œuvre dans tout le Groupe de la Banque mondiale, l'initiative concerne les pratiques et unités mondiales, qui travaillent sur le développement numérique, la protection sociale, la santé, l'inclusion financière, la gouvernance, la parité hommes-femmes et les questions juridiques, entres autres.

L'initiative ID4D se fixe pour mission de donner à tous les individus les moyens d'accéder aux services et d'exercer leurs droits. Elle vise à cet effet à donner une forme officielle d'identification au plus grand nombre, en s'appuyant sur ses trois piliers : i) leadership avisé et analyses pour créer des données probantes et combler les lacunes de connaissances ; ii) plateformes et réunions de niveau international pour donner de l'ampleur aux bonnes pratiques, collaborer et renforcer la sensibilisation ; et iii) engagement national et régional pour apporter l'aide technique et financière nécessaire à la mise en œuvre de systèmes d'identification numérique fiables, inclusifs et responsables, intégrés aux données d'état-civil.

Les travaux de l'initiative ID4D sont rendus possibles avec le soutien du Groupe de la Banque mondiale, de la Fondation Bill & Melinda Gates, d'Omidyar Network et de l'État australien.

Pour en savoir plus sur l'initiative ID4D, visiter id4d.worldbank.org.

Remerciements

Ce rapport a été préparé par Julia Clark, Aziz Ben Ghachem et Yuko Okamura pour le compte de l'initiative « Identification pour le développement » (ID4D) de la Banque mondiale. Le rapport a également grandement bénéficié des commentaires et des contributions de Simon O'Meally, d'Axel Rifon Pérez, de Carlo Rossotto, de Mahdi Barouni, de Julian Najles et de David Satola.

Le rapport n'aurait pas été possible sans les contributions de nombreux membres du gouvernement tunisien qui ont généreusement fourni leur expertise et leur temps pour faciliter cette mission. Citons notamment les membres du Ministère des Technologies de la Communication et de l'Économie Numérique (MTCEN), du Ministère des Affaires Locales et de l'Environnement (MALE), du Ministère des Affaires Sociales (MAS), de la Caisse Nationale de Retraite et de Prévoyance Sociale (CNRPS), la Caisse Nationale de Sécurité Sociale (CNSS), la Caisse Nationale d'Assurance Maladie (CNAM), le Centre de Recherche et d'Etudes Sociales (CRES), le Centre National d'Informatique (CNI), l'Agence nationale de certification électronique (ANCE), la Présidence du gouvernement, le Ministère de la Santé et le Ministère de l'Éducation et l'Instance Nationale pour la Protection des Données Personnelles (INPDP). En outre, le MDICI a contribué au succès de cette mission et à la réalisation du présent rapport.

Les abréviations

ANCE / TUNTRUST : *Agence nationale de certification électronique*

API : *Interface de programmation d'application*

CIN : *Carte d'identité nationale*

CNAM : *Caisse nationale d'assurance maladie*

CNI : *Centre national de l'informatique*

CNRPS : *Caisse nationale de retraite et de prévoyance sociale*

CNSS : *Caisse nationale de sécurité sociale*

CNTE : *Centre National des Technologies de l'Education*

REC : *Registre d'Etat civil*

CRES : *Centre de recherches et d'études sociales*

(e) KYC : *Know Your Customer = Connaissez votre client (électronique)*

INPDP : *Instance nationale de protection des données personnelles*

INS : *L'Institut National de la Statistique*

ISIE : *Instance supérieure indépendante pour les élections*

IS : *identifiant social*

IUC : *Identifiant unique du citoyen*

LPDP : *Loi relative à la protection des données personnelles*

MALE : *Ministère des affaires locales et de l'environnement*

MAS : *Ministère des affaires sociales*

MS : *Ministère de la santé*

MI : *Ministère de l'intérieur*

MTCEN : *Ministère des technologies de la communication et de l'économie numérique*

IDN : *identifiant national*

OGI : *Organe de Gestion de l'IUC*

OTP : *One-time password = Mot de passe à usage unique*

PG : *Présidence du gouvernement*

PKI : *Infrastructure publique principale*

PNAFN : *Programme national d'aide aux familles nécessiteuses*

PNS : *Plan national stratégique*

RIUC : *Registre de l'Identifiant Unique du Citoyen*

UAE : *Unité de l'administration électronique*

UIN : *Unique identity number : Numéro d'identification unique*

Résumé Exécutif

Introduction

Ce rapport présente l'état actuel des systèmes d'identification (ID) en Tunisie et leur utilisation dans différents secteurs. Basé sur une étude initiale réalisée en 2018 par l'Initiative Identification pour le développement (ID4D) de la Banque mondiale, il résume les points forts et les points faibles des principaux systèmes d'identification du pays et fait des recommandations concernant les prochaines étapes sur la voie du développement d'un écosystème d'identification inclusif et fiable qui améliorera la gouvernance et facilitera l'accès aux droits et services de base.

Identification en Tunisie : atouts et lacunes

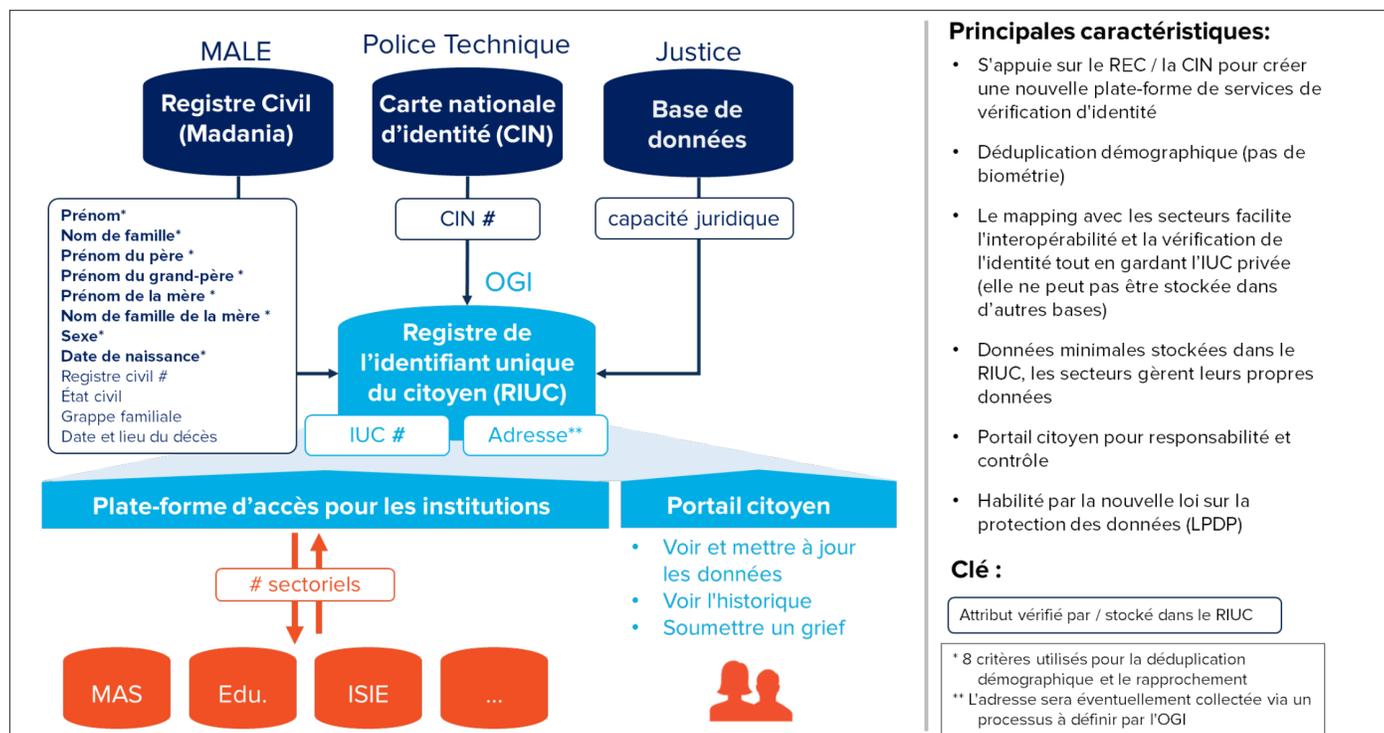
La Tunisie a une longue histoire d'enregistrement et d'identification, et la plupart des gens peuvent prouver leur identité à travers le pays. **Il y a deux systèmes principaux d'« identifiants de base »** : (1) le registre d'état civil (REC), dans lequel le taux d'enregistrement des naissances est de 99%, et (2) une carte d'identité nationale (CIN) détenue par la majorité des citoyens de 18 ans et plus. Malgré la large couverture de ces systèmes et leur robustesse relative, il subsiste des problématiques de qualité des données, de gestion multi lingue, et d'interopérabilité systématique. En outre, aucune de ces méthodes ne fournit un mécanisme d'authentification numérique sécurisé pour les transactions tant présentes qu'en ligne.

En plus de ces systèmes de base, il existe un **nombre de systèmes d'« identifiants fonctionnels »** créés pour un usage sectoriel ou ministériel fournissant une preuve d'identité pour des services spécifiques. Les plus développés d'entre eux sont les registres des diverses caisses d'assurance maladie et de protection sociale contributives et non contributives, qui ont récemment mis en place un numéro d'identification sociale (IS) afin d'améliorer l'interopérabilité et la gestion des enregistrements dans le secteur. En Tunisie, tous les systèmes d'identité fonctionnels s'appuient sur le REC ou bien sur la CIN, dans la mesure où ils exigent des certificats de naissance et / ou des cartes d'identité nationales, dans le cadre du processus d'inscription et de vérification d'identité pour les transactions (par exemple, la perception d'un paiement de sécurité sociale).

Dans le cadre de ses ambitieux plans de transformation numérique - inscrits dans le Plan National Stratégique (PNS), *Tunisie numérique 2020* - Le gouvernement a commencé à mettre en place un nouveau système d'identité afin de créer une « source faisant autorité » d'informations d'identité de base, appelée « **Identifiant unique du citoyen » (IUC)**. Ce système combine les données du registre d'état civil et de la carte d'identité nationale, effectue une déduplication biographique - et non biométrique - et attribue un numéro unique à chaque citoyen, de la naissance jusqu'au décès. Le Registre de l'IUC (RIUC) fonctionnera alors comme un dictionnaire pour faciliter et traduire les requêtes d'identité dans différents secteurs, chacun avec ses propres identifiants qui seront mappés vers l'IUC et stockés dans son Registre. Sur la base de la nouvelle loi sur la protection des données, l'IUC sera uniquement un système « **backend** » et le numéro ne sera pas accessible à d'autres personnes ou à d'autres agences. En raison de cette législation, il sera toujours nécessaire de disposer d'identifiants sectoriels distincts pour se connecter au système IUC.

À l'avenir, différents secteurs seront grandement intéressés par l'utilisation de l'IUC et par la capacité de cet identifiant et de la **plate-forme d'interopérabilité nationale** (TunXRoad) afin d'accroître l'efficacité de l'administration et d'améliorer les services aux citoyens. Cependant, il reste encore beaucoup à faire en termes de vision stratégique et de mise en œuvre technique pour tirer le meilleur parti des systèmes d'identité de base tunisiens à des fins sectorielles.

Schéma 1 . Système d'identification unique projeté



Construire un écosystème d'identification numérique pour la Tunisie : opportunités, défis et recommandations

Globalement, le gouvernement a considérablement amélioré l'identification des citoyens dans le cadre d'une stratégie plus large de transformation numérique, inscrite au PNS. **Les points importants** sont notamment le fait d'atteindre un niveau de couverture élevé des systèmes d'identification de base du pays (c'est-à-dire le registre d'état civil et la carte d'identité nationale), et le fait de fournir des efforts spécifiques dans des domaines prioritaires, tels que la conception et la mise en œuvre de l'IUC, un système informatisé d'enregistrement de l'état civil (*Madania*) et le développement d'un système de protection sociale. La conception du système IUC tunisien comporte un certain nombre de fonctionnalités visant à la protection de la vie privée qui, si elles sont correctement mises en œuvre, pourraient fournir un nouveau modèle dans la région. En outre, le gouvernement met en œuvre ou envisage de nombreux projets connexes visant à développer une infrastructure d'identité numérique, ce qui montre qu'il existe une demande claire de services d'identification, d'authentification et de confiance numérique pouvant répondre aux besoins de divers programmes et utilisateurs.

En même temps, **un certain nombre de lacunes et de défis demeurent**, notamment les problèmes de qualité des données et de manque d'interopérabilité entre les systèmes, les limites des systèmes existants au niveau de l'authentification numérique, les incertitudes concernant la coordination de la redevabilité de la gouvernance du projet et enfin la capacité de mise en œuvre de la nouvelle infrastructure d'identité et de fourniture effective de divers programmes et services. Le présent **rapport fait donc les recommandations suivantes** concernant la manière de tirer parti de ce nouvel élan et de faire en sorte que ces systèmes d'identité répondent aux objectifs du gouvernement et du peuple tunisien :

1. **Mettre en place un comité multi-partis pour synchroniser les projets et fournir une vision globale de l'avenir de l'identification (ID) en Tunisie.** Bien que le PNS donne une vue d'ensemble et que divers projets soient en cours, il n'existe pas encore de vision claire sur la manière dont tous les projets liés à l'identité - par exemple, l'IUC, l'identifiant social (IS), les solutions d'authentification

numérique, TunXRoad – doivent œuvrer ensemble de manière plus coordonnée. Par conséquent, il est essentiel que le gouvernement convoque un groupe plus vaste de parties prenantes qui dresseront un inventaire complet des projets d'identification et d'authentification en cours et travailleront ensemble pour définir une vision plus précise à moyen et long terme, en matière d'infrastructures d'identification et d'authentification. Il est important de noter que le bilan examinera les aspects de la gouvernance et d'administration, afin d'indiquer comment la structure institutionnelle peut être renforcée, à travers le processus de gestion du changement concernant des projets spécifiques (par exemple, l'IUC).

2. **Veiller à ce que la conception de l'IUC se traduise par un système fiable, inclusif et utile.** Le RIUC est envisagé comme un registre d'identité unique qui fournira des services de vérification sécurisés à différents secteurs. Pour que l'IUC puisse jouer ce rôle, sa conception doit être inclusive (couvrir toute la population), acceptée (fiable, sécurisée et responsable), accessible et utile pour une variété d'utilisateurs (personnes et institutions, y compris les ministères sectoriels). Bien que beaucoup de progrès aient été accomplis, des décisions techniques et une planification supplémentaire sont nécessaires pour garantir que le système IUC réponde à ces critères. En outre, l'optimisation des avantages et de l'utilisation de l'IUC dépend des améliorations constantes apportées à la qualité et à la précision de l'état civil (système *Madania*), et de la mise en place d'un cadre national d'interopérabilité qui doivent tous deux être priorisés.
3. **Accélérer le développement de solutions d'authentification numérique.** Malgré les pressions en faveur de l'administration numérique et des services électroniques et l'existence de plusieurs projets liés à l'authentification actuellement en cours, à différents stades de développement, la Tunisie manque actuellement de solutions ou de plateformes numériques qui sont déployées ou adoptées universellement et qui permettant une authentification sécurisée en ligne et présente. Comme indiqué dans la première recommandation, une réflexion plus globale est nécessaire pour faire en sorte que les solutions d'authentification planifiées : (i) répondent aux besoins des différents utilisateurs et des futurs types de transactions ; (ii) soient rentables et interopérables ; et (iii) soient accessibles à l'ensemble de la population.
4. **Renforcer les systèmes d'information et les registres sectoriels lors de la planification de l'intégration aux systèmes nationaux.** Chaque secteur devra continuer à améliorer ses bases de données (registres de bénéficiaires, par exemple) et à mettre au point des systèmes de back-end numérisés et interopérables pour ses programmes et services existants, afin de pouvoir éventuellement se connecter aux systèmes nationaux ou les utiliser (solutions d'authentification numérique, l'IUC, TunXRoad). Dans certains cas, comme la santé, pour lesquels il n'existe pas encore de registre centralisé des patients et d'identifiant sectoriel unique, des investissements importants sont nécessaires. Dans d'autres cas, tels que les secteurs de la protection sociale, des progrès importants ont déjà été réalisés en ce qui concerne la mise en place d'un registre des bénéficiaires, d'un identifiant sectoriel et d'un cadre d'interopérabilité, et il est maintenant possible d'évoluer vers un système plus intégré en y incluant différents programmes sociaux.
5. **Protéger les données et la confidentialité par défaut dès la conception.** La conception du système IUC inclut déjà certains éléments renforçant la protection de la vie privée (par exemple, le fait que le numéro sera privé et non stocké dans d'autres bases de données), qui sont inscrits dans la loi sur la protection des données à caractère personnel (LPDP), actuellement débattue au Parlement. Cependant, pour que ces conceptions réussissent, les parties prenantes doivent veiller à ce que ces réglementations soient bien comprises et appliquées, et à ce que des mesures complémentaires de protection des données et de sécurité par la conception soient intégrées dans tout le système IUC et plus largement dans les systèmes d'identification et d'authentification existants et projetés. En guise de première étape concrète, les impacts sur la vie privée doivent être identifiés. Les mesures d'atténuation doivent ensuite être conçues pour faire face aux impacts négatifs potentiels identifiés, et des mécanismes de contrôle doivent être mis en place lors de la mise en œuvre de ces mesures d'atténuation afin d'assurer la protection des données à caractère personnel lors du processus d'échanges des données entre agences.

PARTIE 1. Introduction

1. Motivation de la présente étude

La Tunisie a une longue histoire d'enregistrement et d'identification, et la plupart des citoyens sont en mesure de prouver leur identité légale. Le cadre juridique et institutionnel de la Tunisie garantit le droit de s'inscrire et d'obtenir une preuve des événements de la vie. L'UNICEF estime que l'enregistrement des naissances est couvert à 99%. De plus, la carte d'identité nationale (CIN) couvre une majorité de citoyens âgés de plus de 18 ans. Le gouvernement tunisien (GT) utilise également divers systèmes d'identification fonctionnels (bases de données, numéros d'identification et cartes) pour identifier la population à des fins spécifiques, notamment des numéros pour les programmes sociaux et l'assurance maladie, un numéro d'identification fiscale, un numéro de passeport, un numéro du permis de conduire et un registre des électeurs.

Cependant, si la couverture de ces systèmes est élevée, aucun d'entre eux ne peut garantir l'unicité et la couverture à 100% de toute la population et ils souffrent de nombreuses inefficacités. En conséquence, de nombreux programmes existants font face à des défis communs pour répondre pleinement aux besoins d'identification et d'authentification de leurs bénéficiaires. Bien que les bases de données soient numériques, le niveau d'intégration et d'interopérabilité est faible. En outre, les procédures permettant aux personnes de demander et de prouver leur identité sont longues. L'authentification pour les transactions de gouvernement à personnes est entièrement manuelle et consiste à donner à l'utilisateur son numéro d'identification (par exemple, un numéro d'assurance sociale) ou à présenter sa carte CIN pour inspection visuelle. À mesure que la Tunisie évolue vers une économie plus numérique, de fortes pressions sont exercées pour créer des plates-formes de services et de transactions en ligne dans les secteurs public et privé.

À cette fin, le GT planifie ou a commencé à mettre en œuvre un certain nombre de projets liés à l'identification. Cela inclut notamment la création d'un numéro d'identification unique (*Identifiant Unique Citoyen*, ou IUC) dans le but de fournir une identification unique tout au long de la vie à tous les Tunisiens et d'améliorer l'interopérabilité et l'intégration des bases de données d'identité. L'IUC - qui est en cours de mise en œuvre - est destiné à soutenir le programme de développement numérique du pays (à savoir, Tunisie Numérique 2020 et le *Plan National Stratégique* ou PNS), simplifier l'administration, réduire les fraudes et les falsifications, et augmenter la transparence et la facilité d'utilisation pour les utilisateurs. Afin d'améliorer l'interopérabilité sectorielle, le Ministère des Affaires Sociales (MAS) a également pris d'importantes mesures pour mettre en place un registre unifié des bénéficiaires afin d'améliorer l'administration et l'exécution des programmes de protection sociale, y compris la mise en place d'un identifiant social. Des projets supplémentaires incluent une plate-forme d'interopérabilité nationale (« TunXRoad »), une carte d'assurance maladie et des services d'administration en ligne qui nécessiteront une méthode d'authentification numérique.

La Banque mondiale ayant soutenu plusieurs projets du GT relatifs à l'identification, la présente étude vise à comprendre l'état actuel des systèmes d'identification en Tunisie dans son ensemble, comme un écosystème couvrant tous les secteurs. Lancées en octobre 2017, une série de premières consultations avec les homologues du GT ont permis d'identifier l'objectif de cette étude, notamment l'utilisation sectorielle des systèmes d'identification pouvant répondre aux besoins du gouvernement et de la population tunisienne en matière de fourniture et de réception des services. Les conclusions initiales de ce rapport ont donc été communiquées aux ministères et départements impliqués, le 19 juillet 2018, et ont servi de

base aux consultations des parties prenantes, tenues en septembre 2018. Ce projet de rapport a également servi à la préparation d'un nouveau projet de gouvernance électronique en Tunisie, financé par un prêt de la Banque mondiale.

Dans l'ensemble, le rapport constate que, si des progrès importants ont été réalisés en matière de développement de systèmes d'information et de déploiement de IUC et de l'IS, il est nécessaire, lors de la prochaine étape, qui doit maximiser le potentiel de ces outils, d'élaborer des plans concrets pour leur développement, leur amélioration et leur adaptation à la fonctionnalité de l'écosystème de l'identification dans son ensemble. Ainsi des efforts supplémentaires demeurent nécessaires pour (1) finaliser la mise en œuvre de l'IUC et du système de gestion associé et s'assurer que les actions de fiabilisation des données soient enclenchées, (2) élaborer un plan concret en vue de prévoir comment l'IUC sera mis à profit par différents systèmes (y compris la mise en correspondance d'identifiants sectoriels avec l'IUC et le potentiel de l'IUC pour faciliter l'interopérabilité des identités entre secteurs), (3) mettre en place un/des système(s) sécurisés d'authentification en ligne et présentiel, pour faciliter les services électroniques et en améliorer l'efficacité, (4) améliorer la coordination des parties prenantes et l'harmonisation des divers projets en cours relatifs à l'identité.

Encadré 1 . Principaux termes liés à l'identité

Une identification ou un **Système d'identification se** compose des *bases de données, des processus, de la technologie, des informations d'identification et des cadres juridiques impliqués dans la saisie, la gestion et l'utilisation de données d'identité personnelle à des fins générales ou spécifiques*. Les principales infrastructures techniques d'un système d'identification sont généralement **les bases de données** (ou registres) de données d'identité et les **identifiants** émis par le système et utilisés par des individus pour prouver leur identité ou des données particulières, tels que des cartes, des codes PIN ou des applications mobiles. De plus, les systèmes d'identification incluent diverses **plateformes** à travers lesquels des tiers peuvent utiliser ces bases de données ou informations d'identification pour vérifier ou authentifier des identités, telles que les couches d'interopérabilité qui facilitent l'échange de données, les requêtes et les transactions liées à l'identité.

En général, les systèmes d'identité peuvent être classés en deux catégories : les systèmes « d'identification de base » et les systèmes « d'identification fonctionnels ». Les **Systèmes d'identification de base** sont créés dans le but de fournir une *identification générale et des justificatifs d'identité à diverses fins* et incluent généralement les registres d'état civil, les cartes d'identité nationales, les registres de population, etc. En revanche, les **systèmes d'identification fonctionnels** sont conçus principalement pour fournir une identification à une fin ou à un secteur spécifique tels que les registres des électeurs, les numéros d'identification fiscale, les registres de protection sociale, les permis de conduire, etc. Les systèmes d'identification fonctionnels gèrent généralement des bases de données dotées de données spécifiques à leur objectif, tels que les scores de pauvreté et les avoirs des ménages pour la protection sociale, ou le revenu annuel pour un système fiscal, et peuvent ou non émettre leurs propres informations d'identité. L'ensemble des systèmes d'identification de base et fonctionnels au sein d'un pays constitue l'**écosystème de l'identité**.

Après une brève explication du rôle de l'identification dans le développement, le reste de ce rapport est organisé comme suit : la 2^e partie fournit une mise à jour sur l'état des projets d'identité et les progrès réalisés depuis l'étude d'évaluation commandée par le GT en 2015 et qui a servi de base au développement de l'IUC. Elle fournit un aperçu des bases de données et des informations d'identification existantes, ainsi que des projets en cours et des problèmes de mise en œuvre. La 3^e partie résume ensuite les principales réalisations, ainsi que les défis et les incertitudes persistantes concernant l'identification en Tunisie, à travers ces différents systèmes et projets, puis fournit des recommandations pour remédier à ces problèmes à l'avenir.

2. Identification pour le développement

Les systèmes d'identification (ID) inclusifs et fiables sont des outils essentiels pour parvenir au développement durable. C'est pour cette raison que le fait de s'assurer que toute personne a accès au système d'identité est inscrit explicitement dans la cible 16.9, de l'Objectif de Développement Durable (ODD), afin de « fournir une identité juridique à tous, y compris au niveau de l'enregistrement des naissances » d'ici 2030. En outre, l'identification est également un facteur essentiel permettant la réalisation de nombreux autres Objectifs de Développement Durable, tels que l'inclusion financière et économique, la protection sociale, les soins de santé et l'éducation pour tous, l'égalité des sexes et une migration sûre et ordonnée, en permettant :

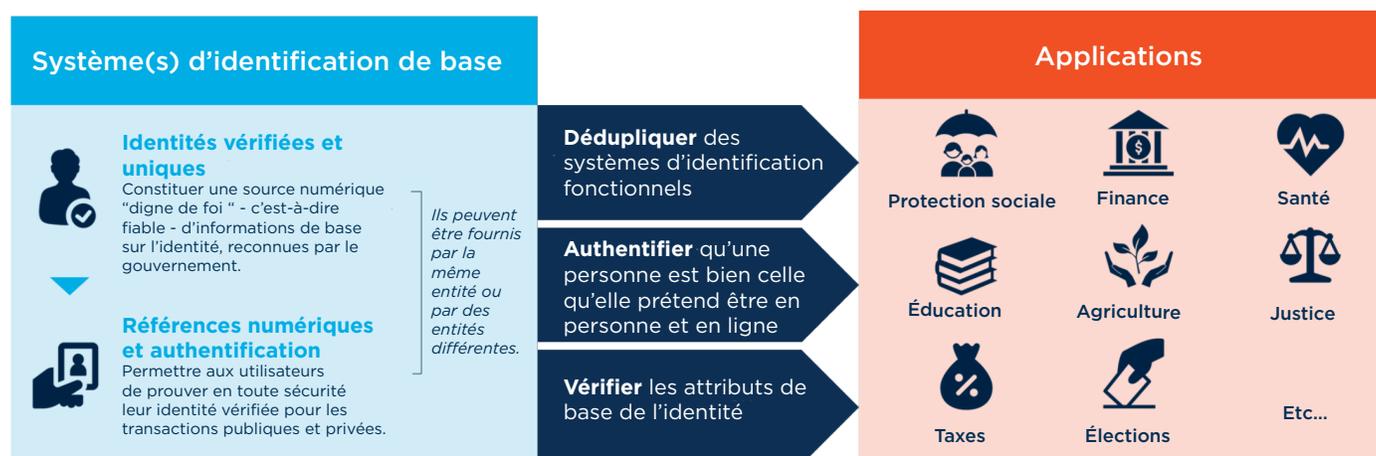
- L'autonomisation des individus et l'amélioration de leur accès aux droits, aux services et à l'économie formelle
- Le renforcement de la transparence, de l'efficacité et de l'efficience de la gouvernance et de la prestation de services
- Le soutien au développement du secteur privé
- La croissance de l'économie numérique
- Le soutien à l'intégration régionale et mondiale

Comme indiqué dans le schéma 1, les systèmes d'identification de base (voir Encadré 1 pour la définition) peuvent remplir deux fonctions importantes au sein de l'écosystème de l'identité et dans divers secteurs :¹

1. **Source fiable d'informations d'identité de base.** En créant un registre d'identités uniques vérifiables, un système d'identification de base peut fournir la base d'une vérification d'identité sécurisée pour les utilisateurs des secteurs public et privé. Dans tous les pays, disposer d'une source fiable d'informations d'identité de base est essentiel à l'intégrité du processus de vérification de l'identité des systèmes d'identité fonctionnels du gouvernement (protection sociale, élections, etc.), des fournisseurs d'identités du secteur privé et des parties utilisatrices (par exemple, des institutions financières ou des opérateurs de réseau mobile effectuant un KYC (Know Your Customer = Connaissez Votre Client). Au-delà de la vérification des éléments d'identité eux-mêmes, un système de base avec des enregistrements d'identité uniques peut également aider à dédupliquer des systèmes fonctionnels - par exemple, un registre des virements monétaires ou une liste de paie publique - réduisant les possibilités de fraude et le besoin de collecte redondante de données par le système de base.
2. **Identifiants numériques et authentification.** En plus d'établir une source d'informations d'identité faisant autorité qui peut être exploitée par d'autres systèmes, les systèmes d'identification de base peuvent également fournir des informations d'identification qui permettent aux personnes d'authentifier leur identité pour une grande variété d'objectifs et de secteurs. Comme pour la vérification, l'authentification peut être un service partagé, fourni à divers utilisateurs des secteurs public et privé. Lorsqu'elle est conçue comme une plate-forme permettant aux utilisateurs d'exploiter les facteurs et mécanismes d'authentification des systèmes d'identification plutôt que de créer leurs propres autorisations (par exemple, via des cadres de fédération ou de reconnaissance mutuelle), cela peut aider à réduire les coûts pour les agences gouvernementales et les entreprises privées.

¹ Pour en savoir plus sur les avantages potentiels et les économies de coûts des systèmes d'identification de base, voir le **Guide du praticien de l'ID4D (Identification pour le Développement)** (<http://id4d.worldbank.org/guide>), Banque mondiale, 2018, *Économies et revenus du secteur public issus des systèmes d'identification : opportunités et contraintes*. Washington, DC : Banque mondiale et Incidences économiques des systèmes d'identification sur le secteur privé, Banque mondiale 2018. Tous deux disponibles à <http://id4d.worldbank.org/research>.

Schéma 2 . L'identité en tant que plateforme de développement



Il est important de noter que, bien que les systèmes d'identification de base fournissent des services de vérification d'identité et d'authentification capables de rationaliser les processus administratifs et d'accroître la sécurité des transactions entre les secteurs, ils ne peuvent remplacer les registres et systèmes d'information sectoriels. Pour respecter les normes internationales en matière de confidentialité et de protection des données, les systèmes d'identification de base ne doivent contenir que les *données minimales* nécessaires, afin d'établir et de vérifier l'identité de base d'une personne et son caractère unique et fournir une vérification et / ou une authentification d'identité de base. En parallèle, différents secteurs maintiennent et exploitent leurs propres registres fonctionnels avec des informations pertinentes et spécifiques à un secteur (dossiers de santé, dossiers d'étudiants, informations sur les avantages sociaux, etc.). Cette séparation des objectifs permet de protéger les données personnelles tout en permettant à un grand nombre d'institutions des secteurs public et privé de tirer parti des services de vérification de l'identité et / ou d'authentification fournis par les systèmes d'identification de base.

Par le passé, la plupart des systèmes d'identification de base (et fonctionnels) étaient en version papier et étaient entièrement gérés par les gouvernements, mais l'identité numérique a brisé ce modèle. Avec le passage à la technologie numérique tout au long du cycle de vie de l'identité, nous avons commencé à voir de nouveaux modèles de partenariats et de cadres fiduciaires entre les gouvernements et le secteur privé pour fournir des solutions d'authentification numérique reconnues par le gouvernement lors des transactions officielles en ligne (par exemple, les services électroniques du gouvernement). Généralement, ces systèmes s'appuient sur les systèmes d'identification de base existants en tant que sources d'information faisant autorité, puis fournissent des services supplémentaires d'authentification et de vérification numériques par le biais de nouveaux canaux (formulaire d'identification mobile, par exemple, Encadré 2 : les Bases de l'authentification).

Encadré 2 . Bases de l'authentification

L'authentification est le processus de vérification de l'identité d'une personne, c'est-à-dire que la personne qui revendique ou « prétend à » une identité particulière est la *même* qui s'est inscrite en premier lieu. Ce processus implique la vérification d'un ou de **plusieurs facteurs d'authentification**, les uns contre les autres, pour voir s'ils correspondent à l'identité revendiquée. Les facteurs d'authentification courants sont notamment :

Quelque chose qu'une personne...

Something a person...



L'authentification numérique — qui utilise des identifiants et des processus électroniques - peut être utilisée pour renforcer la sécurité des transactions **présentielles** (par exemple, en utilisant une carte à puce et un code PIN dans un hôpital). Contrairement aux processus d'authentification analogiques, tels que l'examen de la photo sur la carte d'identité d'une personne, l'authentification numérique peut fournir un beaucoup plus grand **niveau de garantie** (confiance) que la personne est ce qu'elle prétend être. En outre, avec les certificats et signatures numériques, l'authentification numérique permet de sécuriser les transactions **en ligne**, telles que les services électroniques et l'argent mobile.

Différents types de transactions nécessitent différents **niveaux de garantie**, déterminés par la robustesse du processus de vérification de l'identité (vérification de votre identité et de vos pièces justificatives) lors de l'inscription, ainsi que des types de justificatifs d'identité émis et de la technologie utilisée pour l'authentification. Par exemple, une combinaison d'adresse électronique et de mot de passe créée automatiquement fournit un niveau de garantie inférieur à celui d'une pièce d'identité nationale, consistant en une carte à puce, émise après la vérification de l'identité en personne et qui utilise le cryptage PKI et un code PIN pour l'authentification.

Afin d'avoir un impact maximal sur le développement et d'éviter les atteintes à la vie privée, les systèmes d'identification doivent au moins satisfaire aux dix *Principes de l'identification pour le développement durable, indiqué* dans le schéma 2. Ces Principes ont été approuvés par plus de 25 organisations internationales, donateurs, ONG et associations du secteur privé.

Schéma 3 . Principes de l'identification pour le développement durable

Principes	
Inclusion: Couverture Universelle Et Accessibilité	<ol style="list-style-type: none"> 1. Assurer la couverture universelle des personnes de la naissance à la mort, sans discrimination. 2. Supprimer les obstacles à l'accès et à l'utilisation et les disparités dans la disponibilité de l'information et de la technologie.
Conception : Robuste, Sécurisée, Reactive Et Durablee	<ol style="list-style-type: none"> 3. L'établissement d'une identité robuste, unique, sécurisée et précise. 4. La création d'une plate-forme interopérable et qui répond aux besoins des différents utilisateurs. 5. L'utilisation de normes ouvertes et la neutralité du fournisseur et de la technologie. 6. La protection de la vie privée et du contrôle des utilisateurs grâce à la conception du système 7. La planification de la viabilité financière et opérationnelle sans compromettre l'accessibilité
Gouvernance : Construisant La Confiance En Protégant La Confidentialité Et Les Droits Des Utilisateurs	<ol style="list-style-type: none"> 8. La protection de la confidentialité des données, la sécurité et des droits des utilisateurs grâce à un cadre juridique et réglementaire profond. 9. La mise en place de mandats institutionnels et de responsabilités clairs. 10. L'application d'un cadre juridique de confiance à travers un système de surveillance et de traitement des griefs indépendants.
Source: http://id4d.worldbank.org/principles	

PARTIE 2. L'identification en Tunisie : Points forts et Lacunes

Cette section fournit une vue d'ensemble des principaux systèmes d'identification en Tunisie et évalue leurs forces et leurs faiblesses en termes de couverture, de technologie, d'interopérabilité et de gouvernance. Elle commence par une vue d'ensemble de l'écosystème et des principales parties prenantes dans le domaine de l'identification, puis aborde des systèmes d'identification de base et fonctionnels spécifiques (pour le sens de ces termes, voir l'introduction).²

1. Aperçu de l'écosystème d'identité tunisien

Le GT utilise de nombreux systèmes d'identification ayant une couverture élevée au sein de la population. Cela comprend deux systèmes d'« identification de base » utilisés pour fournir une identification générale servant à une grande variété d'objectifs et de transactions : **(1) un registre d'état civil (REC)**, géré par le Ministère des Affaires Locales (MALE) et **(2) une carte d'identité nationale (CIN)**, délivrée par la police technique relevant du Ministère de l'Intérieur. Ensemble, ces deux systèmes fournissent une preuve non électronique d'identité légale à la grande majorité des Tunisiens. Le gouvernement est également actuellement **en cours de mise en œuvre d'un registre d'identités uniques de base** (le RIUC ou *Registre de l'Identifiant Unique du Citoyen*) sur la base des bases de données du REC et de la CIN ; ce registre servira de source d'identité faisant autorité et facilitera les demandes d'identification et l'échange de données entre les organismes gouvernementaux.

En outre, il existe un certain **nombre de systèmes d'« identification fonctionnels »**, conçus pour une utilisation sectorielle par différents ministères, notamment pour la protection sociale et la fiscalité. Le ministère des Affaires sociales (MAS) et les caisses de protection sociale, constituent les parties prenantes les plus importantes de cet écosystème d'identité tunisien, dans la mesure où ils gèrent ensemble des systèmes d'identification couvrant la majorité de la population. D'autres secteurs, tels que la santé, ne disposent pas actuellement de bases de données centralisées sur les bénéficiaires, ni d'identifiants standardisés. Les principaux systèmes, ainsi que leurs organismes fournisseurs, sont résumés dans le Tableau 1.

² Les **Systèmes d'identification de base** sont créés dans le but de fournir une *identification générale et des justificatifs d'identité* à diverses fins et incluent généralement les registres d'état civil, les cartes d'identité nationales, les registres de population, etc. En revanche, les systèmes d'identification fonctionnels sont conçus principalement pour fournir une identification à une fin ou à un secteur spécifique tels que les registres des électeurs, les numéros d'identification fiscale, les registres de protection sociale, les permis de conduire, etc.

Tableau 1 . Vue d'ensemble des principaux systèmes d'identification et registres

	Système	Agence Responsable	Identifiants	Couverture
ID de fondation	Registre d'état civil (REC)	Les collectivités locales, centralisés dans <i>Madania</i> , base de données gérée par le MALE	Actes de naissance, de mariage, de divorce et de décès, livret de famille	99% de la population
	Carte d'identité nationale (CIN)	Police, sous la tutelle du ministère de l'intérieur	Actuellement : CIN #, carte Prévu : CIN électronique, carte à puce	Couverture des adultes environ 90% (estimation)
	En cours : Registre d'identifiant de citoyen unique (RIUC)	Actuellement, le MALE en partenariat avec le ministère de la Technologie (MTCEN) et mis en œuvre par le Centre National de l'Informatique (CNI), sera géré ultérieurement par un organisme de gestion distinct du MALE (l'OGI)	Numéro de citoyen unique (IUC) - il s'agira d'une clé privée utilisateur final, non utilisée lors de l'authentification	~15 millions (couvrant les vivants et les décédés depuis moins de 30 ans - le registre est opérationnel mais tout le système est en cours de mise en œuvre)
Functional ID	Protection sociale et santé	Le Centre de Recherches et d'Etudes Sociales (CRES) du Ministère des Affaires Sociales (MAS) et des caisses de sécurité sociale (CNSS et CNRPS)	Numéro d'identification sociale (IS) [En parallèle, les fonds de sécurité sociale utilisent leurs propres numéros d'identification pour les bénéficiaires antérieurs à la mise en place de l'IS]	10,2 millions, mais certains sont décédés et dupliqués (février 2019)
		Caisse Nationale d'Assurance Maladie (CNAM)	Carte numérique	La distribution a commencé en avril 2019 (pas encore utilisé) ^a
	Taxes	Direction Générale des Impôts	Numéro fiscal	~ 3 millions (c. 2015)
	Registre électoral	Commission électorale (ISIE)	Aucun	5,4 millions (c. Mai 2018) ^b
	Education	Ministère de l'éducation + Centre National des Technologies de L'Education (CNTE)	Identifiant élève	~ 2 millions (c. 2019)

Sources: a. http://www.cnam.nat.tn/doc/upload/fr_com_carte.pdf; b. High Independent Authority for Elections (ISIE), <http://www.isie.tn/electeurs/>.

En plus des fournisseurs d'identité détaillés dans le Tableau 1, il y a un certain nombre d'**autres acteurs importants** dans l'écosystème d'identité tunisien, décrit ci-dessous, dans le Tableau 2. Cela inclut notamment le ministère de la Technologie (MTCEN), qui, en plus de codiriger l'IUC et d'autres projets, héberge le Centre National de l'Informatique (CNI), responsable du développement technique des systèmes RIUC et REC. L'Unité d'Administration Électronique (UAE), au sein du Ministère de la Fonction Publique est responsable des diagnostics, de l'élaboration des politiques et du droit, ainsi que du suivi et de l'évaluation des projets mis en œuvre dans le secteur de l'administration en ligne. L'Instance Nationale de Protection des Données Personnelles (INPDP) joue aussi un rôle important dans la surveillance des programmes d'identité et dans la rédaction de la nouvelle législation sur la protection des données et de la vie privée.

Enfin, L'ANCE (Agence Nationale de Certification Électronique / TUNTRUST) opère une Infrastructure à clé publique (Public Key Infrastructure ou PKI) afin d'assurer un environnement de confiance numérique propice au développement de l'économie numérique. TUNTRUST propose des services de certification et de signature numériques³ et Cachet Electronique Visible pour la sécurisation des documents administratifs via une signature électronique rendue visible à travers un QR Code (code à barre à deux dimensions).⁴ Actuellement, TUNTRUST développe des solutions d'authentification numérique, cependant la couverture et l'utilisation de ces solutions demeurent faibles.

Tableau 2 . Autres acteurs gouvernementaux importants dans l'écosystème d'identité

Entité	Rôle
Ministère de la technologie (MTCEN)	Supervision technique des travaux sur les TIC et les communications en Tunisie, y compris la supervision technique du projet d'IUC et du cadre national d'interopérabilité.
Centre National de l'Informatique (CNI)	Mise en œuvre technique du système REC (<i>Madania</i>) et de l'IUC.
Unité d'Administration Électronique (UAE) du Ministère de la Fonction Publique	Unité chargée des diagnostics, de l'élaboration des politiques et de la législation, de l'intégration des réformes des TIC dans le programme de réformes administratives, du suivi et de l'évaluation de la mise en œuvre des politiques dans le domaine de l'administration électronique, y compris les services électroniques, l'ID et la stratégie Smart Gov (Gouvernement Intelligent)
Agence Nationale de Certification Électronique (ANCE / TUNTRUST)	Fournit des certificats numériques et des signatures électroniques pour certains services
Instance Nationale pour la Protection des Données Personnelles (INPDP)	Organisme indépendant, juridiquement constitué et financièrement autonome, chargé du suivi et de la surveillance des entités qui traitent des données à caractère personnel, y compris les fournisseurs d'identité.

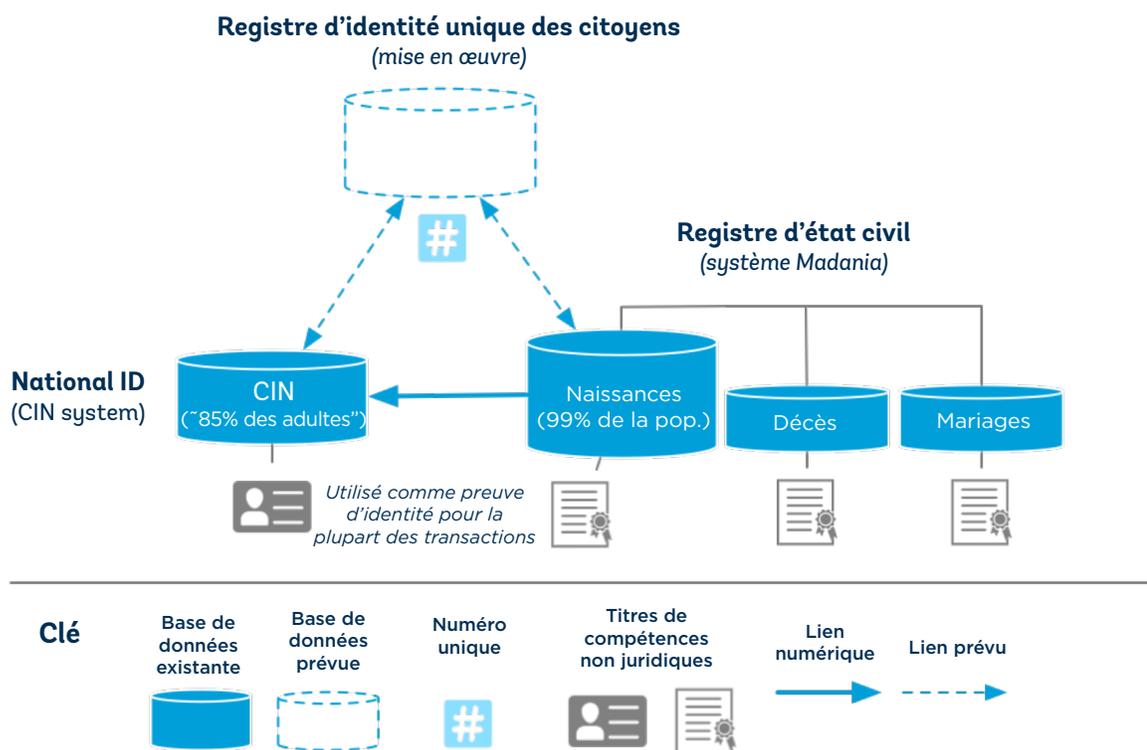
3 Actuellement, les certificats électroniques sont utilisés dans les services e-gov suivants : (1) Tuneps : Achat et marché publics en ligne, (2) Déclaration des taxes en ligne : e-jebaya, (3) Déclaration employeur en ligne : CNSS, CNRPS, (4) Liasse unique pour le commerce extérieur : TTN, (5) Projet facture électronique.

4 Ce service est utilisé pour les diplômes du baccalauréat et de la neuvième année de base, l'extrait du Registre Nationale des Entreprises, et les diplômes universitaires

2. Systèmes d'identification de base

Cette section couvre, de manière détaillée, les **deux principaux systèmes d'identification de base, en Tunisie - le registre d'état civil et la CIN**. Elle décrit également le **registre de l'identifiant unique des citoyens (RIUC)**, qui fait partie du PNS (voir Schéma 3). Le RIUC devrait moderniser les systèmes d'identité du pays en facilitant les services de vérification de l'identité et l'interopérabilité entre diverses bases de données sectorielles. Toutefois, le projet n'en est encore qu'à ses débuts et son déploiement est prévu pour 2021.

Schéma 4 . Systèmes d'identification de base en Tunisie



Le Registre d'Etat Civil (REC)

La Tunisie possède un système solide d'enregistrement des actes d'état civil qui, sous sa forme moderne, date du début du XXe siècle. Après l'indépendance, une loi sur l'état civil a été adoptée en 1957, rendant obligatoire l'enregistrement des naissances et des décès et établissant le droit d'obtenir la preuve des faits essentiels d'état civil.⁵ L'enregistrement civil - y compris l'enregistrement des naissances, l'enregistrement des décès et des contrats de mariage - est réalisé par les collectivités locales constituées principalement des 350 municipalités (communes) du pays, bien que d'autres organes administratifs locaux (délégations) aient également exercé ces activités dans les zones rurales jusqu'en 2018.⁶

⁵ Voir le texte de loi à l'adresse <https://www.jurisitetunisie.com/tunisie/codes/csp/civil1000.htm>.

⁶ Auparavant, il y avait 264 municipalités qui ne couvraient que les zones urbaines du pays. Les résidents des zones rurales s'adressaient plutôt aux agents administratifs de leur délégation (*mouatamdeya*) pour les mêmes services. Cependant, à partir de 2016, de nouvelles municipalités ont été créées (et les anciennes ont été élargies) pour couvrir l'ensemble du territoire de façon permanente, de sorte que l'ensemble de la population est désormais sous la juridiction d'une municipalité et de son conseil élu.

Afin d'effectuer l'enregistrement des naissances, les parents doivent se rendre service de l'état civil au siège de la municipalité et présenter les documents relatifs à la naissance (ex : certificat médical), la preuve de l'identité de la mère et du père (carte d'identité nationale, CIN) et une signature. L'enregistrement est gratuit, mais doit être effectué dans les 10 jours suivant la naissance, ou bien est considéré comme un enregistrement tardif et doit ensuite être effectué devant un tribunal (le tribunal de première instance).⁷ L'enregistrement des décès suit un processus similaire et doit être effectué dans les trois jours suivant le décès. L'UNICEF estime dans l'ensemble que l'enregistrement des naissances est réalisé à 99% (voir Tableau 3).

Tableau 3 . Couverture de l'état civil

Registre d'état civil	Inscription
Population cible	Tous les résidents en Tunisie et les citoyens tunisiens vivant à l'étranger
Taille de la population cible	11,4 millions personnes en Tunisie (2016)
Obligatoire ?	Oui, dans les 10 jours suivant la naissance
Couverture totale*	Actes enregistrés (personnes vivantes et décédées) à partir de 2018 : 18,53 millions de naissances 4,14 millions de décès 3,8 millions de mariages
Taux d'enregistrement des naissances **	99 pour cent
Source : * MALE (2019), ** ID4D Global Dataset, 2018 (les données originales concernant l'enregistrement des naissances proviennent de l'UNICEF, vers 2016).	

Base de données et intégration du REC

Les événements civils sont enregistrés au niveau municipal dans des registres physiques. Les données sur les naissances, les décès et les mariages sont ensuite entrées manuellement dans le système d'information de l'état civil, appelé *Madania* ("Civil" en arabe), par des responsables locaux. Le système a été déployé pour la première fois en 1992 par le CNI, dans la municipalité de Tunis, puis déployé à l'échelle nationale à partir de 2004.⁸ En 2015, il était accessible à partir de près de 481 sites (toutes les municipalités ainsi que des sites régionaux et commerciaux) et de 1 300 postes de travail à travers le pays, et utilisé par environ 1 500 personnes.

Avant la numérisation du REC et le développement de *Madania*, en arabe et en français, les personnes devaient se rendre au lieu où l'acte civil avait été enregistré à l'origine (par exemple, leur lieu de naissance) pour demander des copies des certificats délivrées en se référant aux registres papier. Avec le système *Madania*, ils peuvent désormais se rendre à n'importe quel bureau municipal et demander des copies de documents ou corriger les erreurs. Dans le cas de mises à jour, ces modifications sont signalées à la municipalité où l'événement a été enregistré originellement et sont ensuite modifiées dans le registre physique, puis téléchargées dans la base de données.

Les renseignements sur les différents événements (naissances, décès et mariages) sont conservés séparément au sein du système *Madania*, sans liens systématiques entre eux. Ainsi, ce système ne peut pas servir de registre de la population, avec un processus d'enregistrement unique pour chaque individu. Cependant, un projet en cours visant à améliorer la qualité des données (voir ci-dessous) mettra en place des contrôles et des recoupements plus systématiques entre les bases de données.

⁷ Source : <http://www.collectiviteslocales.gov.tn/etat-civil/>.

⁸ <https://www.webmanagercenter.com/2005/05/16/11728/Madania-2-un-projet-de-e-gouvernement/>

Tableau 4 . Attributs stockés dans la base de données d'enregistrement des naissances Madania

Type	Attributs	Type de collecte
Biographiques	<ol style="list-style-type: none"> 1. Prénom 2. Nom de famille 3. Date de naissance 4. Lieu de naissance 5. Sexe 6. Chaîne de noms de père (prénom du père + prénom du grand-père) 7. Date de naissance du père 8. Lieu de naissance du père 9. Profession de père 10. Nationalité du père 11. Chaîne de noms de la mère (prénom de la mère + prénom du grand-père + nom de famille de la mère) 12. Date de naissance de la mère 13. Lieu de naissance de la mère 14. Profession de la mère 15. Nationalité de la mère 16. Nom, âge, profession du déclarant 	Entré dans un registre papier, puis entré manuellement dans la base de données de Madania.
Métadonnées	<ol style="list-style-type: none"> 1. Date de déclaration 2. Prénom du fonctionnaire qui a traité la demande 3. Nom du fonctionnaire qui a traité la demande 	
Biométriques	Aucun	n.d.

Actuellement, il existe peu de liens automatisés entre *Madania* et d'autres systèmes (voir Tableau 5). Dans la plupart des cas, les ministères ou autres entités autorisés peuvent demander une copie de certaines informations, qui sont envoyées au format numérique sur un support physique. Cependant, le gouvernement est en train de mettre en place des services pour faciliter les requêtes automatisées du système *Madania*.

Par exemple, le système « e-madhoun » permet l'échange d'extraits de naissance entre organismes gouvernementaux via une plate-forme Web gérée par le CNI. Le premier projet pilote de ce système s'est fait avec le ministère de l'Éducation (voir la section ci-dessous sur les systèmes d'identification fonctionnels) et des applications sont en cours de développement pour couvrir le secteur social (MAS), le Ministère de l'Emploi et Formation professionnelle et le Ministère de l'Enseignement supérieur.

Tableau 5 . Stockage et transfert de données de Madania

Registre d'état civil	Base de données CR (Madania)
Architecture de base de données	3 bases de données séparées (et non connectés) sur les naissances, les décès et les mariages / divorces, réparties en: locale → régionale → centrale
Bases de données avec lesquelles le système échange des informations	Échange de données avec : <ul style="list-style-type: none"> • Le Ministère de l'éducation (via la plateforme e-E-madhmoun) • CNRPS (au besoin) via un fichier texte et un serveur FTP (depuis Mars 2019 échange via E-Madhmoun) • CNSS (au besoin) via un fichier texte et un serveur FTP (depuis Mars 2019 échange via E-Madhmoun) • ISIE pour les élections • L'Institut National de la Statistique (INS) pour les statistiques démographiques • Les synchronisations se produisent par lots et de nuit, pendant cette opération la base de données est indisponible.
Technologie de base de données	Serveur SQL, 18Go
Sauvegarde et reprise après sinistre	Serveur de sauvegarde avec DSI au ministère de l'Intérieur

Le principal défi concernant le nettoyage de la base de données du REC et son intégration à d'autres systèmes a été le format d'enregistrement des noms en arabe et en français. Actuellement, les noms de famille en arabe, y compris les noms du père et du grand-père, sont saisis en tant que champ unique de type "chaîne". Compte tenu de la structure des noms arabes (les prénoms et les noms de famille étant souvent des mots composés), le chaînage rend difficile la réconciliation avec d'autres sources de données. En outre, la transcription des noms arabes et leur saisie en alphabet latin varie souvent de manière significative.

Outre les problèmes de langue, il existe d'autres problèmes liés à l'exactitude des données dans le système, telle que la double entrée des naissances. En 2015, environ 300 000 doubles déclarations de naissances avaient été détectées au total dans le système. Par ailleurs, les enregistrements relatifs aux Tunisiens à l'étranger, ne sont entrés que chaque 6 mois, ce qui retarde la mise à jour du système. En outre, comme les enregistrements des naissances, des décès et des mariages sont conservés dans différentes bases de données, il est possible que des erreurs soient commises et que des données d'identité soient incohérentes dans les trois systèmes d'enregistrement. Enfin, le numéro de référence du registre *Madania* est assez long (20 chiffres) et n'inclut pas les sommes de contrôle, ce qui entraîne de fréquentes erreurs de transcription.

Certificats et Numéros

Les principaux certificats délivrés par le REC sont les certificats et les numéros de références (utilisés pour localiser l'acte) de naissance, de décès et de mariage, ainsi que le livret de famille. Les actes de naissance, extraits et livrets de famille sont couramment utilisés comme preuve d'identité et d'état civil à diverses fins, souvent en combinaison avec la CIN (pour les adultes). Tous les certificats sont en version papier et incluent des numéros de référence codés avec le lieu et la date de délivrance (voir Schéma 4 et Tableau 6). Cependant, bien que le numéro de l'acte civil soit fréquemment enregistré dans d'autres bases de données (par exemple, dans les caisses d'assurance sociale), certains contrôles visant à vérifier la naissance d'une personne sont effectués en comparant huit données principales - prénom, nom de famille, date de naissance, sexe, prénom du père, prénom du grand-père, prénom de la mère et nom de famille de la mère - aux données du système *Madania* , plutôt que d'utiliser le numéro lui-même.

Schéma 5 . Structure du numéro de référence du REC (Madania)



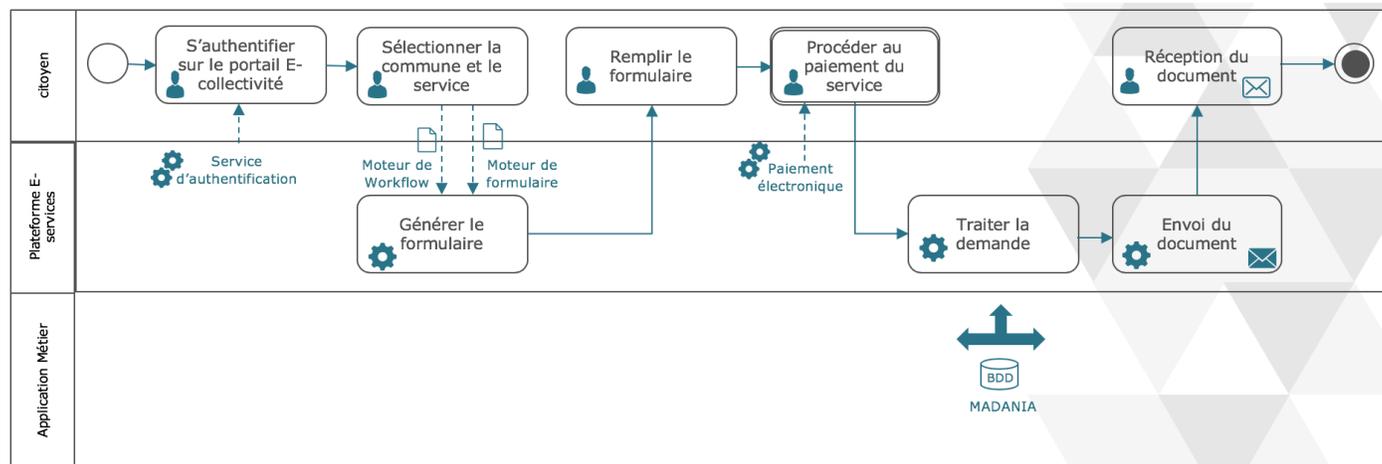
Tableau 6 . Certificats et extraits de naissance

Registre d'état civil	Certificat et extrait de naissance
Lors de l'émission	Lors de l'enregistrement de la naissance, des copies supplémentaires (extraits) peuvent être demandées plus tard
Coût	Premier exemplaire gratuit, 0,5 DT (USD 0.18) ensuite
Expiration	Permanent, toutefois, pour certains services (par exemple, l'obtention d'une carte CIN), l'extrait doit être récent (généralement moins de trois mois).
Type et format du numéro de référence	20 chiffres, codés avec : <ul style="list-style-type: none"> • Municipalité (commune) [4 chiffres] • District / arrondissement [2 chiffres] • Registre consulaire [1 chiffre] • Localité [2 chiffres] • Type de registre [2 chiffres] • Année [4 chiffres] Acte d'enregistrement des naissances [5 chiffres - série séquentielle locale qui commence à 0 chaque nouvelle année]
Le numéro des personnes décédées est-il recyclé?	Non, car les chiffres incluent l'année d'émission
Matériel	Certificats papier
Lisibilité machine	<i>Actuellement</i> : Aucun <i>Projeté</i> : Les certificats / extraits seront imprimés avec des codes QR
Temps pour émettre	Délivré sur place si la demande est complète.
Méthode de collecte	En personne (peut être collecté par un parent, un enfant ou le conjoint de la personne), ou par la poste (la personne doit se présenter et avoir une pièce d'identité pour récupérer le document). Il est également possible de faire la demande en ligne et de la récupérer en personne via https://www.etatcivil.gov.tn/Madania/web/indexfr (partiellement opérationnel depuis 2018).

Étant donné que des copies récentes de l'extrait de naissance sont généralement requises pour les processus administratifs, il est souvent nécessaire d'obtenir des versions mises à jour de ces documents. Auparavant, cela nécessitait une visite en personne dans un bureau municipal. Cependant, à compter de 2018, le MALE - en coopération avec le MTCEN, le CIN et la Poste tunisienne - a mis en place un service qui permet aux personnes de demander une copie de leur acte de naissance (extrait *de naissance*) en ligne via <https://www.etatcivil.gov.tn/> en utilisant leur numéro CIN. Une fois la demande complétée et le paiement effectué, des copies papier des certificats sont envoyées par courrier au domicile du demandeur en Tunisie ou à l'étranger, et livrées après vérification de leur CIN. Cependant, bien que le service puisse éviter aux citoyens de se déplacer jusqu'à l'administration municipale - ce qui est particulièrement pratique pour

les Tunisiens à l'étranger - à plus long terme, l'objectif est de réduire le nombre de services nécessitant que les personnes présentent leur acte de naissance en mettant en œuvre des requêtes automatisées de vérification des informations dans l'état civil (par exemple, comme avec e-madhmoun et par l'RIUC comme décrit ci-dessous).

Schéma 6 . Demande de services en ligne projetée pour des certificats de naissance demande en ligne



Source : MALE.

Plans de réforme du système Madania

Le MALE, le MTCEN et le CNI ont mis au point une stratégie pour améliorer le système *Madania* qui résoudra certains des problèmes d'intégration et de qualité des données décrits ci-dessus. Dans l'ensemble, l'objectif n'est pas seulement d'améliorer les performances du système actuel, mais également de faire de *Madania* une plate-forme moderne qui répond aux besoins de plusieurs parties prenantes. Les objectifs spécifiques, en sont notamment de :

- Faciliter l'interopérabilité du système *Madania* avec l'IUC, la CIN, le CNSS, le CNRPS et éventuellement d'autres ministères et organismes publics (par exemple, ministère de la Santé, le ministère de la Défense, le ministère de l'Éducation, le ministère de l'Enseignement supérieur, l'agence nationale de la statistique)
- Passer à un système sans papier qui réduit le contact physique entre les citoyens et l'administration
- Améliorer la qualité et l'exactitude des données, notamment en « déliant » les noms de famille (par exemple, les prénoms du père et du grand-père) et en reliant les différents enregistrements du REC (naissance, mariages / divorces et décès)
- Détermination des grappes familiales - c.-à-d. relier les membres de la famille dans la base de données
- Fournir aux organismes publics concernés (hôpitaux, ministère de l'éducation, INS) des informations statistiques
- Encourager les échanges électroniques sécurisés entre les bureaux des REC au niveau municipal
- Améliorer la sécurité et la confidentialité des données (notamment par le cryptage et une solide authentification)
- Passer à une architecture orientée vers les services, les technologies ouvertes et l'indépendance vis-à-vis des technologies payantes
- Développer une plate-forme d'interopérabilité, des services électroniques et des services mobiles

Selon les plans actuels, le système sera développé en 2020 et déployé en 2021.

Carte d'identité nationale (CIN)⁹

La carte d'identité nationale (ou CIN) est l'autre système d'identification de base en Tunisie et on estime qu'il couvre une large majorité de la population des citoyens adultes. Les cartes sont émises à partir de 18 ans¹⁰ et servent de preuve d'identité pour presque toutes les transactions (voir Tableau 7).

Tableau 7 . Couverture de la CIN

Carte d'identité nationale	CIN
Population cible	Pour les citoyens, obligatoires à 18 ans mais peut être obtenue avant
Taille de la population cible (18+)	8,3 millions (c. 2018) ^a
Population cible couverte	Taux de couverture aux environs de 90% ^b
Sources :	
a. ID4D Global Dataset, disponible à l'adresse http://id4d.worldbank.org/global-dataset .	
b. Les chiffres précis seront insérés après réception des données du ministère de l'Intérieur. Selon certaines sources d'information, la couverture serait d'environ 7 millions (~ 84% des adultes de 18 ans et plus), alors que selon d'autres, seuls 300 000 adultes ne seraient pas porteurs du CIN. Voir par exemple : https://www.huffpostmaghreb.com/2018/01/03/carte-didentite-biometriq_n_18926246.html et https://www.espacemanager.com/chafik-sarsar-300-mille-tunisiens-nont-pas-de-cartes-didentite.html .	

Le système est géré par la police technique du ministère de l'Intérieur, et les Tunisiens demandent et renouvellent leur carte d'identité auprès des postes de police locaux ou des bureaux de la garde nationale de leur lieu de résidence. Pour pouvoir demander une CIN, une personne doit fournir un extrait de naissance délivré au cours des trois derniers mois (voir ci-dessus), un certificat de nationalité tunisienne, un certificat de résidence, un certificat de travail ou un statut d'étudiant, un certificat du groupe sanguin (facultatif), une empreinte de pouce encrée et trois photos. Après avoir rempli une demande, la police est censée délivrer la carte dans les 15 jours suivants.¹¹ La demande initiale de carte coûte 3 TND (1 USD), tandis que les remplacements de cartes perdues ou volées coûtent 25 TND (9 USD).¹²

Tableau 8 . Administration de CIN

Carte d'identité nationale	CIN
Fournisseur d'identifiant	Police technique, Ministère de l'intérieur
Bureaux et responsabilités	<ul style="list-style-type: none"> • Postes de police locaux et bureaux de la garde nationale : traiter les demandes • 31 bureaux régionaux : Saisie manuelle des données, émission du numéro de CIN, impression de carte • Administration centrale : Validation et archivage des données, gestion globale

Carte CIN

La version actuelle du CIN est une carte plastique basique, avec un code à barres lisible par machine ; elle est émise depuis 1993 (Schéma 7), remplaçant les cartes en papier stratifié précédemment émises (Schéma 8). En 2014, les anciennes cartes n'étaient plus valables.¹³ Cependant, environ 350 000 cartes papier étaient toujours en circulation en 2015. Au cours des dernières années, environ 700 000 CIN nouvelles ou de remplacement ont été émises chaque année, et environ 21 millions de nouvelles cartes et cartes de remplacement ont été émises entre 1993 et 2015¹⁴, pour une population d'environ 11,5 millions d'habitants.

9 Remarque : cette section n'a pas reçu les données du ministère de l'Intérieur / et de la Police technique et doit être vérifiée.

10 Les cartes peuvent être exceptionnellement fournies aux personnes de moins de 18 ans, ce qui nécessite une documentation supplémentaire de la part du tuteur légal, y compris la raison pour laquelle la carte est nécessaire. <http://services.interieur.gov.tn/wap/fr/docs/demarches/01.html>.

11 <http://services.interieur.gov.tn/wap/fr/docs/demarches/01.html>.

12 <https://directinfo.webmanagercenter.com/2012/12/28/tunisie-la-cin-a-25-dt-et-le-passeport-a-150-dt/>

13 <http://mag14.com/actuel/35-societe/705-tunisie-precisions-sur-le-nouvellement-des-cartes-didentite.html>.

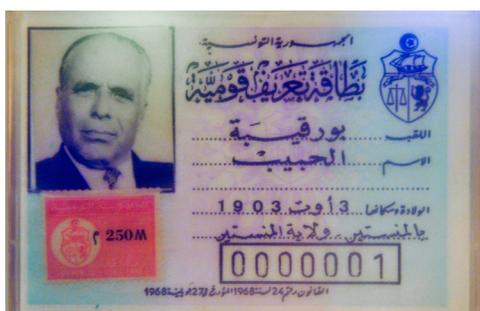
14 <http://opendata.interieur.gov.tn/fr/catalog/les-cartes-d-identite-nationale-et-bulletins-n-3-fournis-par-la-direction-de-la-police-technique-et-scientifique-durant-les-annees-2014-2015>.

La carte n'est pas électronique et, par conséquent, les procédures d'authentification utilisant cette carte n'impliquent qu'une vérification manuelle.

Schéma 7 . Nouvelle CIN (après 1993)



Schéma 8 . Ancienne CNI remise au premier président tunisien, Habib Bourguiba



Source: Citizen59 (CC BY-SA 3.0)

Tableau 9 . Carte et numéro CIN

Carte d'identité nationale	CIN
Première émission	1993
Délivrée quand et à qui	Citoyens adultes, 18 ans et plus
Expiration	Aucun ^a
Matériel	En plastique
Lisibilité machine	Code à barres
Données lisibles par l'homme	Nom, prénom, prénom du père, prénom du grand-père, prénom et nom de la mère, date de naissance, résidence, profession, adresse, date CIN émise, image de l'empreinte numérique, numéro CIN et chiffres de contrôle
Données lisibles par machine	Numéro de la carte stocké dans le code à barres
Numéro CIN	8 numéros séquentiels, avec différentes plages dans différentes régions (si une région est vide, les plages sont transférées à une autre)
Cryptage	Aucun
Personnalisation des cartes	Bureaux régionaux
Processus de demande	En personne
Méthode de collecte	En personne
Temps pour émettre	La police passe environ 15 jours pour traiter une demande. Toutefois, une personne aura probablement besoin d'au moins deux semaines pour obtenir les documents (certificat de résidence, certificat de nationalité, etc.) nécessaires pour demander la CIN. Il est donc probable que la procédure prendrait en moyenne un mois pour l'ensemble du processus.

Source : a. http://www.sicad.gov.tn/Fr/Renouvellement-de-la-carte-didentite-par-une-carte-didentite-nationale_57_3_D1310.

Base de données et intégration de la CIN

Au cours du processus d'inscription, les formulaires papier en arabe et les pièces justificatives sont rassemblés au niveau local, puis envoyés aux bureaux régionaux (voir Tableau 10). Là, des informations biographiques sont entrées dans la base de données et traduites en français, ainsi que des données biométriques (empreinte digitale encrée et photo). Une fois le numéro CIN attribué, les données et les pièces justificatives sont envoyées au niveau central pour rapprochement et stockage. Après validation des données, les cartes sont ensuite imprimées au niveau régional.

Tableau 10 . Données et documents requis pour l'obtention de la CIN¹⁵

Exigences de la CIN	Type	Collecte	Validation	Stockage
Documents à l'appui	Certificats de naissance, de nationalité, de résidence, profession et groupe sanguin (facultatif) ; le cas échéant, certificats de mariage ou de décès du conjoint en cas de veuvage	Formulaires papier collectés	Inconnu	Enregistrements papier stockés dans les archives centrales
Données biographiques (saisies en arabe, traduites en français)	Nom, prénom, nom du père, nom du grand-père, date et lieu de naissance, prénom et nom de la mère, sexe, situation de famille (célibataire, marié, veuf), prénom et nom du conjoint, profession, adresse actuelle, groupe sanguin (facultatif) et si donneur de sang	Formulaire papier, entré manuellement dans l'ordinateur	Sur la base des pièces justificatives	Base biographique centrale
Données biométriques	3 copies d'une photographie, empreinte(s) de pouce encrée(s), signature physique	Formulaire de candidature, numérisé ensuite	Inconnu	Base de données centrale pour les images biométriques

Les données ne sont pas dédoublées lors du renouvellement, il est donc possible qu'une personne ait plusieurs cartes / numéros de CIN et, dans certains cas, plusieurs personnes peuvent avoir le même numéro CIN. En 2015, on a estimé à environ 2 500 le nombre de cartes doubles. En outre, un certain nombre de champs de données, notamment l'adresse et la profession, sont souvent obsolètes.

Tableau 11 . Stockage et transfert de données pour la CIN

Carte d'identité nationale	CIN
Architecture de base de données	Deux bases de données : (1) informations biographiques (le donne sur la carte plus autres (par exemple : le nom et prénom de l'épouse si le citoyen est marié), (2) informations biométriques (images numérisées d'empreintes digitales et de photos)
Bases de données avec lesquelles le système échange des informations	ISIE : Avant les élections, le système de la CIN remet une liste de citoyens à la commission électorale. <i>Madania</i> : Sur demande, le REC fournit des informations sur l'état civil et / ou le décès d'une personne, ce qui implique l'échange physique d'un fichier texte.

15 Besoin de vérifier avec le Ministère de l'Intérieur.

Technologie de base de données	Biographique : développé en interne sous Cobol, utilise le système d'exploitation VSE-CICS et la gestion de fichiers VSAM Biométrique : solution clé en main
Centres de sauvegarde et de reprise après sinistre	Sauvegarde des données biométriques sur un serveur de le Centre Informatique du Ministère de l'Intérieur

Projets pour la CIN

Le ministère de l'Intérieur (Mdl) a élaboré des plans en vue de la délivrance d'une nouvelle version de la CIN ; sous la forme d'une carte à puce biométrique, appelée eCIN. La proposition initiale incluait une carte avec une micropuce qui contiendrait une photo et l'empreinte digitale droite du détenteur de la carte, qui ne pouvait être accessible que par la police et la garde nationale responsables de la vérification de l'identité. La carte et / ou la puce contiendrait également des données similaires à celles de la CIN actuelle, y compris les noms et prénoms du titulaire de la carte, de leurs parents, de leur grand-père paternel, l'adresse et le numéro de la CIN, ainsi que des données facultatives, y compris le nom et le prénom du conjoint, un groupe sanguin et si la personne est un donneur d'organes. Le coût du projet s'élèverait à quelque 40 millions de dinars (14,6 millions de dollars).

En 2016, un projet de loi organique a été présenté à l'Assemblée nationale (ARP), modifiant l'ancienne législation régissant la CIN (loi n ° 9327 du 22 mars 1993) pour faciliter le projet eCIN. Cependant, le projet a été retiré début 2018 en raison d'inquiétudes concernant la vie privée. Bien que l'instance nationale pour la protection des données personnelles (INPDP) ait apporté son soutien à l'authentification biométrique via une carte à puce, elle s'est dit préoccupée par les risques de sécurité associés au développement d'une base de données biométrique centralisée. En outre, l'INPDP et des militants de la société civile ont fait part de leurs préoccupations concernant le fait que les données stockées sous forme cryptée sur une puce ne seraient accessibles que par la police, violant ainsi le droit des citoyens à la surveillance et à la transparence sur les personnes qui ont accès à leurs informations.¹⁶ À partir de fin 2019, le Mdl envisage toujours d'introduire un eCIN, mais aucun projet de législation révisée n'a été présenté.

¹⁶ <https://www.webmanagercenter.com/2018/01/10/414655/arp-le-gouvernement-retire-le-projet-de-loi-sur-la-carte-didentite-biometrique/>, <https://www.nessma.tv/fr/article/polemique-autour-de-la-carte-d-identite-biometrique-3180>, https://www.huffpostmaghreb.com/2018/01/03/carte-didentite-biometriq_n_18926246.html, <https://thd.tn/tunisie-sommes-nous-prets-a-la-carte-didentite-biometrique/>, <https://africanmanager.com/tunisie-les-empreintes-de-85-millions-de-tunisiens-ne-seront-pas-securisees-alerte-le-president-de-linpdp/>.

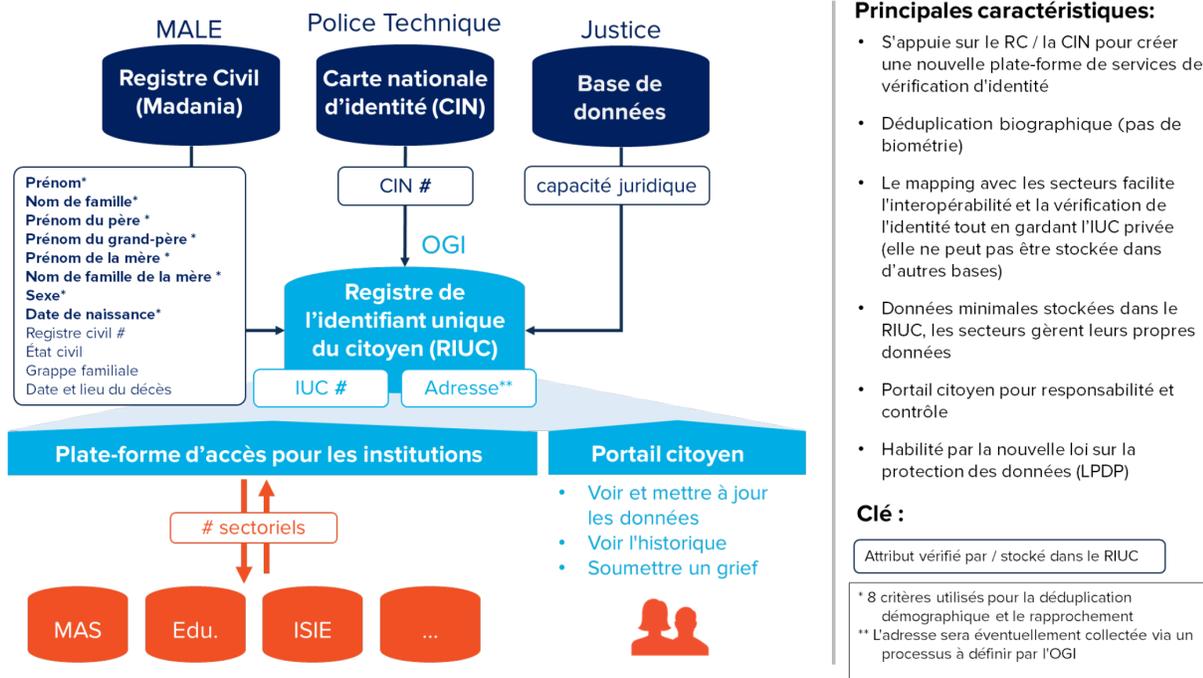
Projets de « l'identifiant unique de citoyen (IUC) »

La composante e-gouvernement du Plan national stratégique (PNS) « *Tunisie numérique 2020* » appelle à la transformation de l'administration publique grâce à l'adoption de la technologie numérique qui augmentera l'efficacité et la transparence pour les citoyens et les entreprises. Cet objectif était motivé par (1) l'existence de multiples identifiants sectoriels et d'une infrastructure informatique hétérogène limitant les échanges de données entre départements, (2) l'inexactitude des données d'identité dans les systèmes de base et ceux fonctionnels, et (3) la nécessité d'améliorer la gestion administrative et de rationaliser les services publics fournis aux citoyens.

Afin de concrétiser ces objectifs, le PNS a appelé à la création d'un *identifiant unique citoyen* (IUC) - conjointement avec le développement des services électroniques et un cadre national d'interopérabilité. La planification de l'IUC a débuté en 2015 avec une première étude réalisée pour le compte du ministère de la Technologie (MTCEN), qui a permis d'élaborer le plan préliminaire de l'IUC. Un comité de pilotage composé de parties prenantes a été formé et, en 2017, le MALE (titulaire du projet), le MTCEN et l'INPDP ont signé un protocole d'accord concernant les rôles et le modèle de gouvernance du projet. Depuis lors, ces trois organisations, ainsi que le système de la CNI, ont continué à progresser dans la définition de la conception technique et des plans de mise en œuvre de l'IUC.

La vision actuelle est de créer un système de référence national - c'est-à-dire un registre et un dictionnaire - qui représente une « source faisant autorité » d'informations sur l'identité d'une personne et qui peut être utilisé pour faciliter l'échange de données dans le secteur public. Le système validera les données d'identité de base pour tous les citoyens, en puisant dans les systèmes de la CIN et du REC, émettra un numéro IUC et stockera ces informations dans un système intitulé **Registre d'identifiant unique de citoyen** (ou **RIUC**). En outre, le système comprendra des plates-formes permettant aux administrateurs publics d'interroger la base de données et un portail d'accès citoyen pour la surveillance de leurs données (voir Schéma 9).

Schéma 9 . Système d'IUC projeté



Conception

L'IUC sera un **enregistrement d'un numéro de référence backend stocké uniquement dans la base de données RIUC** et ne sera pas inséré ni stocké dans d'autres bases de données (comme c'est le cas en Inde, en Estonie et dans d'autres pays). Plutôt que d'incorporer l'IUC dans des systèmes sectoriels, les identifiants sectoriels seront mappés à l'IUC dans la base de données RIUC. Il s'agit d'une conception délibérée - inscrite dans la législation habilitante de l'IUC - visant à protéger la vie privée en limitant la prolifération (et l'utilisation abusive potentielle) du numéro unique.

Dans cette architecture, il semblerait que le RIUC facilitera la vérification de l'identité et la communication entre les systèmes sectoriels en jouant le rôle de traducteur central. Par exemple, si le secteur social a besoin de vérifier l'inscription d'un enfant à l'école, il peut envoyer une demande au RIUC avec l'identifiant social, qui le mapperait sur l'identifiant de l'élève, afin de faciliter la recherche. Grâce à cette fonctionnalité, le système IUC peut potentiellement aider à rationaliser et simplifier la gestion de divers registres d'identité, à réduire le nombre de fraudes et à simplifier les procédures administratives pour les citoyens, tout en limitant la diffusion de l'IUC lui-même.

Bien que le système n'ait pas encore été complètement mis en œuvre, un certain nombre de décisions essentielles ont déjà été prises concernant la gouvernance, la couverture, le développement de la base de données RIUC, les procédures de déduplication, le format du numéro IUC et les services fournis par différents secteurs. Certains de ces choix ont été spécifiés dans la nouvelle loi sur la protection des données qui servira de base à l'IUC, tandis que d'autres ont été définis par les directeurs du projet.

Lois habilitantes

Les caractéristiques techniques ainsi que la gouvernance du système IUC seront largement définies par une nouvelle loi organique, la loi sur la protection des données à caractère personnel (LPDP), qui a été soumise à l'Assemblée nationale en mars 2018 et qui fait l'objet d'un débat au parlement depuis juin 2019.¹⁷ La LPDP - traitée plus en détail à la section IV - actualisera la législation générale en vigueur sur la protection des données en Tunisie, afin de refléter le droit à la vie privée dans la nouvelle constitution, clarifiera les zones d'ombre et harmonisera la législation tunisienne avec les nouvelles normes de données européennes (à savoir la Convention 108+, à laquelle la Tunisie a adhéré en 2017, et le GDPR).¹⁸ En outre, elle comprend une législation spécifique habilitante pour l'IUC, qui est résumée dans l'encadré 3. Comme spécifié dans l'article 75, des spécifications plus détaillées du système seront publiées par décret gouvernemental.

17 Débat au sein de la Commission des droits et libertés et des relations extérieures : http://arp.tn/site/projet/EN/fiche_proj.jsp?cp=101988

18 L'article 24 de la Constitution de 2014 stipule que « L'État protège la vie privée, l'inviolabilité du domicile et le secret des correspondances ».

Encadré 3 . Articles liés à l'identification dans le projet de loi sur la protection des données

Dans sa version actuelle, il existe plusieurs articles en relation directe avec l'IUC (les traductions sont effectuées par les auteurs et ne sont donc pas validées), citons-en les suivants.

Article 75 : Un « registre de l'identifiant unique du citoyen » sera créé, par un décret gouvernemental qui en définira les objectifs et fixera les données personnelles qui seront concernées. Il sera maintenu et géré par le MALE.

Article 76 : La tenue et la gestion du registre IUC sont soumises aux mêmes conditions et modalités que celles applicables à la gestion des données à caractère personnel, et les personnes autorisées à utiliser l'IUC sont tenues de faciliter les audits conduits par l'INPDP et, à ce titre, de désigner un responsable de la protection des données.

Article 77 : L'IUC est attribué à (i) toute personne inscrite à la naissance au REC [registre d'état civil] (ii) toute personne de nationalité tunisienne née dans un pays étranger et enregistrée auprès de la mission diplomatique ou consulaire de ce pays (iii) toute personne ayant acquis la nationalité tunisienne. Les données associées à ces personnes doivent être conservées 30 ans après le décès ou la perte de la nationalité.

Article 78 : Il est interdit d'attribuer le même IUC à plus d'une personne et d'attribuer plus d'un IUC à une personne. Le code IUC ne doit pas contenir d'informations d'identification. Ses objectifs, son contenu, ses caractéristiques techniques et les règles de maintenance et de gestion de son registre seront définis par décret gouvernemental, après consultation de l'INPDP.

Article 79 : Il incombe au MALE de mettre en place un système en ligne permettant à tous les citoyens de prendre connaissance de toutes les opérations en rapport avec leur IUC et des institutions qui l'ont utilisé.

Article 80 : L'utilisation de l'IUC est interdite sauf par des agents publics ou privés chargés de la gestion d'un établissement public et qui sont fondés à utiliser l'IUC selon les termes dudit décret gouvernemental, après consultation de l'INPDP.

Article 81 : Il est interdit d'imprimer l'IUC sur des documents officiels délivrés par les services de l'Etat tunisien, à l'exception de la correspondance administrative entre les structures publiques ou privées mentionnées dans l'article précédent.

Gouvernance et supervision

Le MALE est le chef du projet (*maître d'ouvrage*) du développement du RIUC dans son ensemble, en partenariat étroit avec le MTCEN, qui assure la direction technique du bureau de gestion de projet (BGP), et avec le CNI, chargé de la mise en œuvre de la base de données et des systèmes d'information. Le pilotage stratégique du projet est assuré par le comité de pilotage (COFIL), qui est également dirigé par le MALE et comprend des membres de diverses parties prenantes, notamment le MTCEN, le CNI, l'INPDP, le Ministère de l'Intérieur, le Ministère de l'Administration publique, l'Institut National de la Statistique (INS), le Ministère des Finances, le MAS, etc. Un comité opérationnel (COOP) dirigé par le MTCEN se réunit tous les mois pour superviser et valider les décisions techniques. Il est composé de représentants de MALE, de l'INPDP, de l'INS, du CNI, du MAS, du Ministère de la Santé, du Ministère de l'Éducation et du Ministère de l'Intérieur. En outre, un groupe de travail technique - composé du MALE, du MTCEN et du CNI - se réunit toutes les semaines, et d'autres groupes de travail ad hoc sont convoqués, selon les besoins, pour traiter de problèmes techniques spécifiques.

La structure de gouvernance existante est destinée à la phase de démarrage uniquement. Ultérieurement, un « organe de gestion » de l'IUC (*Organe de Gestion de l'IUC*, ou OGI) sera créé pour gérer l'IUC. Bien que les paramètres organisationnels et opérationnels de l'OGI n'aient pas encore été définis, il est actuellement prévu de le loger au sein de la Direction Générale de l'Informatique du MALE. L'INPDP continuera de jouer un rôle de supervision pour l'IUC, notamment en accordant son approbation à la liste des utilisateurs du système et en effectuant à cette fin des audits (articles 76 et 80 de la LPDP, voir ci-dessus).

Couverture

Selon l'article 77 du LPDP, l'IUC sera attribué à la naissance et couvrira tous les Tunisiens résidant en Tunisie, les citoyens naturalisés et les citoyens tunisiens résidant à l'étranger. Étant donné que le RIUC utilisera à la fois les enregistrements de la CIN et du REC, il devrait couvrir une large majorité de la population existante en raison de la couverture élevée de ces systèmes combinés. Cependant, il n'est pas clair si des efforts particuliers seront entrepris afin d'inscrire le petit pourcentage de Tunisiens qui n'ont jamais été enregistrés à la naissance et qui n'ont pas de CIN¹⁹ et, si oui, quelle forme prendrait ce processus.²⁰ En outre, il n'est pas prévu dans l'immédiat d'inclure des résidents étrangers ou d'autres ressortissants étrangers dans le système afin de faire du RIUC un véritable « registre de la population ». ²¹ Cependant, la police des frontières exploite une base de données de résidents en Tunisie qui pourrait être intégrée à l'avenir. En outre, le numéro IUC a été structuré de telle manière que le chiffre le plus à gauche (un « 0 » pour les inscriptions initiales des citoyens) puisse être utilisé pour désigner les non-nationaux à l'avenir.

Les citoyens resteront dans la base de données du RIUC, avec un numéro unique pour toute leur vie et durant 30 ans après leur décès ou la perte de leur nationalité tunisienne. Ensuite, leurs données seront anonymisées ou supprimées (LPDP Article 77) ; toutefois, un registre des IUC attribués aux décédés sera conservé indéfiniment pour s'assurer qu'ils ne sont pas réaffectés.

Base de données RIUC

Le CNI a piloté l'initialisation de la base de données RIUC en nettoyant et en dédoublant les copies des attributs de la CIN et de *Madania* (voir Tableau 12), puis en harmonisant les deux. En février 2018, la base de données contenait environ 14 millions d'enregistrements comprenant des citoyens vivants et des personnes décédées au cours des 30 dernières années. Une fois le projet pleinement mis en œuvre, il établira des liens permanents avec les deux systèmes afin que le RIUC reste informé des nouvelles (1) naissances, (2) décès, (3) structures familiales (mariages, divorces et enfants), (4) des modifications apportées aux informations REC et (5) des nouveaux numéros de la CIN. En outre, le RIUC sera relié à une base de données du Ministère de la justice afin de synchroniser les données liées au statut juridique et inclura une correspondance des numéros IUC avec les identifiants sectoriels (processus à définir également) afin de faciliter les requêtes d'identité intersectorielles. Éventuellement, les personnes pourront déclarer elles-mêmes leur adresse dans le système, mais ce processus n'a pas encore été défini.

19 Bien que on ne connaisse pas le nombre exact de personnes qui ne sont pas enregistrées dans les systèmes d'identité de base du pays, extrapoler à partir du taux d'enregistrement de naissance déclaré par l'UNICEF de 99% signifierait qu'environ 115 000 enfants de moins de 5 ans qui n'étaient pas enregistrés à la naissance. De même, si nous supposons une couverture du CIN de 90% (probablement une estimation prudente, voir la section précédente), cela pourrait signifier qu'environ d'un 830 000 d'adultes tunisiens ne possèdent pas la carte. Bien que ces chiffres puissent être relativement faibles, ce sont souvent les couches de la population les plus marginalisées et les plus vulnérables qui n'ont pas de carte d'identité (par exemple, les femmes rurales pauvres, etc.) et qui peuvent être exclues de l'accès aux programmes nécessitant une preuve d'identité.

20 Les citoyens qui ne figurent pas dans la base de données de *Madania*, mais qui possèdent une CIN ne seront pas inclus dans l'initialisation du système RIUC. Cependant, ils seront identifiés dans un « dossier d'anomalies » et inclus plus tard après un processus d'adjudication. Cependant, il ne semble pas y avoir de plan concret sur la manière d'inclure les ressortissants qui ne figurent ni dans *Madania*, ni dans la base de données de la CIN (voir note précédente).

21 Au début, le projet de la LPDP n'a pas fait référence seulement aux citoyens, mais à ceux qui sont inscrits dans l'état civil. Cependant, le texte a depuis été modifié pour ne faire référence qu'aux citoyens. Dans les plans d'initialisation de la base de données RIUC, les non-citoyens possédant des enregistrements dans le système *Madania* (c'est-à-dire que leurs naissances, leurs décès ou leurs mariages ont été enregistrés) seront initialement exclus, dans l'attente de projets ultérieurs d'incorporation de non-ressortissants.

Tableau 12 . Données à stocker dans le RIUC (en arabe et en français)

Catégorie	Données	Source
Biographique	Nom * + Prénom * + Prénom du père * + Prénom du grand-père paternel * + Nom de famille de la mère * + Prénom de la mère * + Sexe Date de naissance * + Lieu de naissance + Etat civil et IUC du conjoint actuel IUC des parents et des enfants (clusters familiaux) Date de décès Lieu de décès	<i>Création de la base de données : REC (Madania) / Base de données de la CIN à sommer et à harmoniser.</i> <i>Nouveaux inscrits et mises à jour : déclenché à partir du REC (Madania)</i>
	Adresse déclarée	À partir d'auto déclarations, validées via un processus à définir par l'OGL.
Numéros d'identité	Numéro IUC	<i>Généré après déduplication et rapprochement des données REC et CIN</i>
	Numéro de référence du certificat de naissance +	<i>REC (Madania)</i>
	Année du numéro de référence du certificat de naissance +	
	Numéro de la CIN	Base de données CIN
	Identifiants sectoriels (par exemple, IS, numéro d'identification fiscale) <i>matricule fiscale</i> , etc.)	Bases de données sectorielles (processus à définir)
Situation légale	Actes et décisions relatifs à la capacité juridique	Ministère de la justice
* Huit attributs utilisés pour la déduplication + Données confrontés et harmonisés avec ceux de la CIN		

Déduplication

Compte tenu de la taille relativement petite de la population tunisienne (moins de 12 millions) et des préoccupations liées à la confidentialité, les responsables de la mise en œuvre ont choisi la déduplication biographique plutôt que biométrique. Un algorithme de déduplication repose sur huit attributs principaux : nom de famille, prénom, nom du père, prénom du grand-père, prénom de la mère, nom de famille de la mère, date de naissance et sexe.²² Grâce à ce processus, le système IUC assurera **une identification statistiquement unique** de la population (article 78 de la LPDP) en ce sens que :

22 Ces critères ont été utilisés pour dédupliquer la base de données *Madania*, avant la confrontation avec la base de données de la CIN ; des mesures supplémentaires ont également été prises pour dédupliquer les données CIN, avant la confrontation (par exemple, suppression des personnes ayant plusieurs numéros CIN, etc.).

- Tous les citoyens inscrits dans *Madania* auront un IUC, sauf ceux décédés 30 ans avant l'initialisation de la base de données.
- Aucun citoyen ne peut avoir plus d'un IUC, même s'il a deux certificats de naissance.
- Chaque IUC est assigné à un seul citoyen, pour toute la vie et 30 ans après son décès.

Numéro IUC

L'IUC sera un numéro à 11 chiffres, composé d'un préfixe à un chiffre, d'une racine séquentielle à 8 chiffres (non-aléatoire) et de deux numéros de contrôle, comme indiqué dans le Schéma 10. Initialement, le préfixe était destiné à indiquer si la personne avait une CIN. Dans la conception actuelle toutefois, 0 sera assigné à tous les ressortissants tunisiens. Si le système devait être élargi à l'avenir pour inclure des non-nationaux, l'idée serait de structurer leurs numéros IUC en commençant par 1.

Schéma 10 . Structure prévue du numéro IUC



Comme décrit ci-dessus, **le numéro IUC est destiné à rester privé**. Selon l'article 81 de la LPDP, il ne peut être visible sur aucun document officiel, tel qu'un acte de naissance ou une carte d'identité. En conséquence, il ne sera pas connu des gens ou utilisé directement pour l'authentification (par exemple, comme dans le système indien Aadhaar). Il s'agit plutôt d'une clé unique stockée dans le système RIUC, qui servira principalement de plate-forme pour la vérification d'identité back-end.

Les services

Les utilisateurs - y compris les divers organismes et ministères, ainsi que les personnes elles-mêmes - accéderont au système RIUC via deux mécanismes :

- **Plateforme d'accès pour les institutions publiques et privées :** les entités publiques et privées, impliquées dans la fourniture de services publics, pourront accéder à certaines données à travers une plateforme d'accès sur la base d'accords de partenariat avec l'OGI (article 80 du LPDP). Cette plate-forme sera liée à la plate-forme d'interopérabilité nationale (TunXRoad) et conçue pour répondre à un certain nombre d'exigences, y compris des transactions sécurisées avec un accès contrôlé, des pistes d'audit et une neutralité technologique nécessitant une adaptation minimale de la part des utilisateurs.
- **Portail d'accès citoyen :** Les personnes pourront consulter leurs données personnelles et leur utilisation via un portail en ligne (article 79 de la LPDP). Ce portail remplira un certain nombre de fonctions, notamment en permettant aux citoyens de mettre à jour leurs certaines données, de consulter l'historique des consultations et de préciser comment elles ont été utilisées.

Initialement, les services principaux rendus par la plate-forme IUC comprennent la vérification de la vie, le partage des données d'identité de base pour préremplir les formulaires et la vérification des données de base et des identifiants, comme indiqué dans Tableau 13. Comme décrit ci-dessus, l'objectif final est également que le RIUC serve de dictionnaire permettant à différents systèmes fonctionnels d'échanger des informations via leurs propres identifiants distincts.

Tableau 13 . Liste des premiers services développés pour le RIUC

Service	Description	Premiers clients
<p>Consultation des données de décès</p>	<p>Ce service permet de consulter les informations concernant les décès des affiliés et ce en se basant sur les mentions de décès figurant dans l'acte de naissance et les actes de décès (du <i>Madania</i>). Ce service va épargner au citoyen la fourniture d'actes état civil à l'administration pour prouver qu'il est encore en vie et optimiser de la gestion des droits.</p> <p>Données en entrée :</p> <ul style="list-style-type: none"> • Tous : commune de naissance, date de naissance, sexe, nom, prénom, prénom père, prénom mère, nom mère, prénom grand père • Ou Identifiant Social (IS) • Ou référence de l'acte de naissance <p>Données en sortie :</p> <p>Renvoie une réponse indiquant si la personne est vivante ou décédée et, en cas de décès, la date et le certificat de décès.</p>	<p>MAS, CNSS, CNRPS, CNAM)</p>
<p>Consultation des données biographiques</p>	<p>Ce service permet de consulter les données de l'acte de naissance d'un citoyen. Il peut être utilisé pour : (1) pré-rendre les données d'identification de base (réduisant le risque d'erreur de saisie de données), (2) vérifier que les données des bases de données interrogées correspondent à la personne et / ou (3) compléter les informations manquantes dans la base de données auteur de la requête. Ce service va épargner au citoyen la fourniture de l'acte de naissance à l'administration.</p> <p>Données en entrée :</p> <ul style="list-style-type: none"> • Tous : commune de naissance, date de naissance, sexe, nom, prénom, prénom père, prénom mère, nom mère, prénom grand père • Ou Identifiant sectoriel (Identifiant Social, Identifiant élève, etc.) • Ou référence de l'acte de naissance <p>Données en sortie : nom, prénom, chaîne père, chaîne mère, date de naissance, genre.</p>	<p>Ministère de l'éducation nationale : Inscription des élèves</p> <p>MAS/CNSS/CNRPS/ CNAM : affiliation</p>

Consultation de la situation familiale d'un citoyen	<p>Ce service permet de consulter les informations concernant la situation familiale des affiliés. Ce service va épargner au citoyen la fourniture d'actes état civil à l'administration pour prouver qu'il est encore en vie et optimiser de la gestion des droits.</p> <p>Données en entrée :</p> <ul style="list-style-type: none"> • Tous : Commune de naissance, date de naissance, sexe, nom, prénom, prénom père, prénom mère, nom mère, prénom grand père • Ou Identifiant Social (IS) • Ou référence de l'acte de naissance <p>Données en sortie : Situation familiale (marié, non marié), date de mariage si marié</p>	MAS, CNSS, CNRPS, CNAM
Consultation des données concernant le conjoint d'un citoyen	<p>Ce service permet de consulter les informations concernant le (la) conjoint(e) d'affilié(e). Ce service va épargner au citoyen la fourniture d'actes état civil à l'administration.</p> <p>Données en entrée :</p> <ul style="list-style-type: none"> • Tous : commune de naissance, Date de naissance, sexe, nom, prénom, prénom père, prénom mère, nom mère, prénom grand père • Identifiant Social (IS) • Référence de l'acte de naissance <p>Données en sortie : nom et prénom du conjoint</p>	MAS, CNSS, CNRPS, CNAM
Source : MALE et MTCEN.		

Chronologie

- 2017 : Lancement du projet IUC.
- 2019 :
 - Une première version du système d'information IUC (avec un RIUC comportant près de 15 millions d'enregistrements) est entrée en production en septembre 2019 permettant l'accès aux données du RIUC aux systèmes d'information de la MAS, CNRPS, CNAM, CNSS et l'éducation (via les services aux Tableau 13).
 - Lancement du processus de passation de marché pour le développement et le déploiement d'une version plus élaborée du système d'information IUC.
 - Lancement du processus de passation de marché pour la refonte du système national de gestion de l'état civil (*Madania*), source principale des données du RIUC.
- 2020 : Implémentation et déploiement des nouveaux systèmes IUC et *Madania*
- 2021 : Mise en production et exploitation à grande échelle du système IUC et *Madania*.

Parallèlement, des efforts sont en cours pour accroître la précision de la base de données RIUC initialisée et pour identifier les doublons et les erreurs dans les données source (bases de données *Madania* et de la CNI). Une fois ce rapprochement terminé - prévu pour 2020 ou le début de 2021 -, les bureaux d'enregistrement locaux organiseront une campagne visant à améliorer la fiabilité de leurs données, prévue pour 2020-2024, parallèlement à la refonte du système *Madania*.

3. Systèmes d'identification fonctionnels

Outre les systèmes de base décrits ci-dessus, le gouvernement tunisien exploite également un certain nombre de systèmes d'identification fonctionnels à usage sectoriel. Ces systèmes jouent un rôle essentiel dans l'identification de la population éligible pour un service, un droit ou une procédure administrative particulière (par exemple, les bénéficiaires de transferts monétaires, contribuables, électeurs, etc.) et, dans certains cas, émettent leurs propres identifiants ou pièces d'identité pour l'authentification. Les systèmes d'identification fonctionnels les plus développés et les plus étendus en Tunisie sont ceux utilisés pour gérer les programmes de protection sociale du pays. Cette section fournit une analyse approfondie de divers systèmes de protection sociale, ainsi que des aperçus de l'identification dans d'autres secteurs, notamment la santé, l'éducation, et la fiscalité.

Protection sociale

Aperçu du secteur

Le système de protection sociale tunisien comprend des programmes non contributifs (c.-à-d. des programmes d'assistance sociale / des filets de protection sociale) et des programmes contributifs (c.-à-d. la sécurité sociale, y compris le retraite et l'assurance maladie)

- Il existe deux principaux programmes d'assistance sociale non contributifs, notamment un programme de transfert monétaire appelé Programme National d'Assistance aux Familles Nécessiteuses (*Programme d'Aide aux Familles Nécessiteuses*, ou PNAFN) et un programme d'assurance maladie pour les indigents appelé AMG 1/2.²³ Ces programmes sont administrés par le Ministère des Affaires Sociales et concernent actuellement environ 30% de la population.
- Pour le système contributif, il existe deux caisses de sécurité sociale, une pour le secteur privé (Caisse nationale de sécurité sociale, ou CNSS) et l'autre pour le secteur public (Caisse *nationale de retraite et de prévoyance sociale* ou CNRPS). Ces fonds de sécurité sociale sont responsables de la collecte des cotisations et du traitement des paiements des pensions, des prestations aux veuves et des orphelins des retraités, des prestations de décès et des prêts sociaux. Bien que la couverture des systèmes de retraite soit élevée, environ 50% de la main-d'œuvre actuelle contribue à l'un des deux principaux systèmes de sécurité sociale.²⁴

Par conséquent, toutes les personnes inscrites à la CNSS et à la CNRPS sont automatiquement admissibles au programme national d'assurance maladie, administré par la caisse nationale d'assurance maladie (CNAM)²⁵. Si l'on y ajoute les bénéficiaires du programme d'aide sociale, on estime qu'environ 90% de la population est couverte par des programmes d'assurance maladie en Tunisie.

Le MAS, la CNSS, le CNRPS et le Centre de recherche et d'études sociales (CRES) ont déployé des efforts concertés pour moderniser le système d'exécution de ces programmes de protection sociale, notamment

23 Le PNAFN est destiné à la population la plus pauvre, couvrant environ 8% de la population. En plus d'un transfert d'argent, les bénéficiaires de la PNAFN ont également accès à des soins de santé gratuits dans les établissements publics (AMG1, *Assurance médicale gratuite de type 1*). 22% supplémentaires de la population vulnérable qui ne peut pas faire partie du système d'assurance maladie contributif reçoivent une carte santé subventionnée (AMG2 ou *Carnet de soin à tarif réduit*), leur permettant d'avoir accès aux soins médicaux dans les établissements de santé publique en payant un forfait annuel fixe.

24 Banque mondiale (2019). *Revue des dépenses publiques en Tunisie*.

25 La CNAM a été créée en 2007 dans le but d'unifier divers régimes d'assurance et de prestations de santé et d'accroître la couverture des services de santé par des prestataires privés. Elle propose des régimes d'assurance maladie, des régimes d'indemnisation des accidents du travail (*Accidents de travail et maladie professionnelle* ou ATMP), prestations de maladie fournies par les régimes de sécurité sociale et autres formes d'assistance.

en améliorant les registres et l'identification des bénéficiaires. Les principales actions engagées ont été les suivantes :

- Développer et améliorer les **systèmes de gestion de l'information du MAS** et des caisses de **sécurité sociale** , y compris la mise en place d'un **identifiant social (IS) et d'une plate-forme d'interopérabilité** pour la gestion de l'identité et l'échange de données entre régimes non contributifs et contributifs.
- Développer une **base de données des bénéficiaires** mise à jour des principaux programmes de protection sociale (PNAFN et AMG2) qui pourrait jeter les bases d'un futur **registre social unifié** et permettre la conception d'un outil de ciblage.
- Émettre une **nouvelle carte (gérée par la CNAM)** pour améliorer l'authentification des bénéficiaires dans les hôpitaux en remplaçant les cartes papier actuelles.

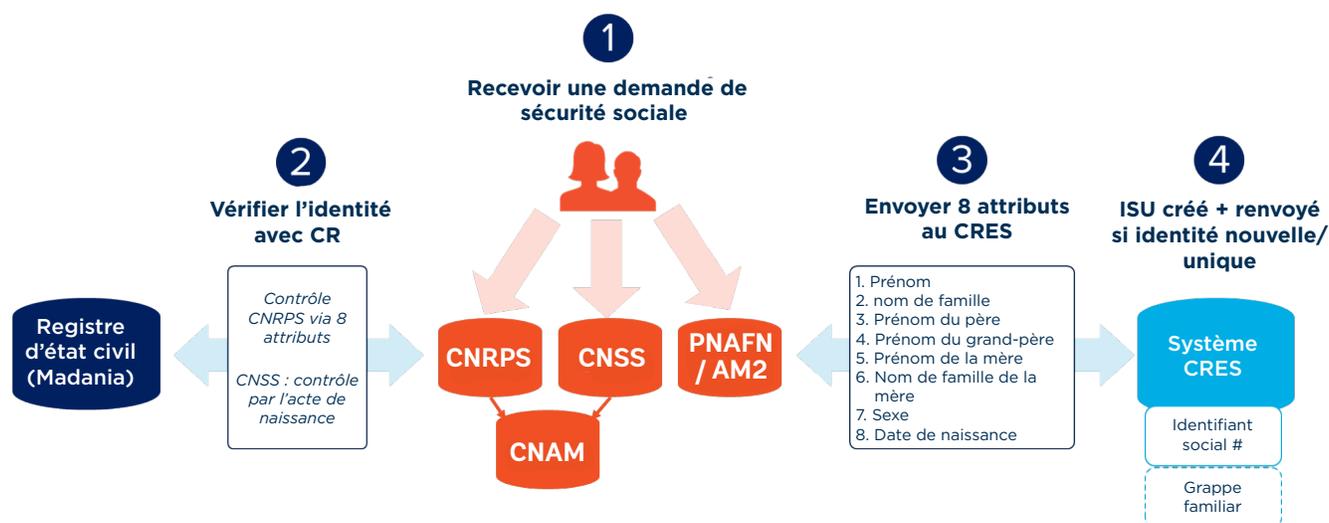
La section suivante traite en détail deux de ces projets : l'identifiant social (IS) et la carte CNAM.

Identifiant social (IS)

L'objectif initial et principal de l'IS est d'identifier les individus des systèmes contributifs et non contributifs afin d'améliorer le ciblage des programmes d'aide sociale. Concrètement, avec l'IS, le MAS peut vérifier plus efficacement la cotisation du bénéficiaire du filet de sécurité sociale, à la sécurité sociale. Le projet IS a débuté en 2003, sous la forme d'une collaboration entre les deux caisses de sécurité sociale (CNSS et CNRPS). Il a ensuite été étendu à la CNAM, ainsi qu'aux programmes de protection sociale non contributifs gérés par le MAS. Le système informatique est exploité par le CRES, qui émet des numéros uniques ²⁶ pour chaque bénéficiaire à travers les programmes sociaux, sur la base des données fournies par le MAS, la CNSS et la CNRPS.

L'IS a été attribué à plus de 10 millions d'individus (à compter de mai 2019), la CNSS constituant la principale source de la base de données (environ 80% des données proviennent de la CNSS). Ce nombre inclut les personnes qui ne sont plus actives et implique la possibilité de duplication de l'enregistrement. Pour améliorer le processus et les données, un audit du système d'information a été réalisé en 2019 et les recommandations devraient être mises en œuvre.

Schéma 11 . Génération de l'IS



26 À terme, le CRES envisage également de regrouper les familles - c'est-à-dire les liens entre les identités des membres de la famille - qui sont nécessaires pour cibler les programmes de protection sociale en fonction des ménages. Il n'est pas clair si cela pourrait tirer parti de plans similaires conçus pour le système *Madania*.

Comme indiqué dans Schéma 11, la CNSS, la CNRPS et le MAS transmettent leurs données au CRES, y compris les huit critères détaillés dans le Tableau 14 — qui sont notamment les mêmes critères utilisés pour dédupliquer les citoyens dans le RIUC. Le CRES utilise ces informations pour dédupliquer les bénéficiaires et déterminer si un IS a déjà été attribué à un individu donné (par exemple, comme cela se produit lorsqu'une personne change de secteur d'emploi). Le CRES génère ensuite le numéro IS (ou trouve un numéro existant) et le renvoie à la base de données des caisses. L'application du CRES contient un algorithme de contrôle faisant référence à un dictionnaire de noms/prénoms en arabe pour éviter les problèmes de transcription.

Tableau 14 . Résumé de l'IS

Identifiant social (IS)	
Couverture	Les bénéficiaires du programme d'assistance sociale et les membres de leurs familles Contributeurs aux systèmes de sécurité sociale et les personnes à leur charge
Nombre d'individus ayant un IS (réel)	10,8 millions en mai 2019 (87% de la population du pays) <ul style="list-style-type: none"> - 8,1 millions de la CNSS (79% de la base de données) - 1,7 million de CNRPS (14% de la base de données) +1 million du MAS (7% de la base de données) [Ce nombre devrait atteindre 2 millions lorsque le MAS aura terminé de mettre à jour les informations de tous les bénéficiaires du PNAFN et de l'AMG1 / 2]
Données biographiques	Huit critères sont nécessaires pour dédupliquer l'identité d'une personne et générer l'IS : <ol style="list-style-type: none"> 1. Prénom 2. Nom 3. Prénom du père 4. Prénom du grand-père 5. Prénom de la mère 6. Nom de famille de la mère 7. Date de naissance 8. Sexe <p>En outre, les informations suivantes sont collectées, le cas échéant : (9) adresse, (10), état civil (célibataire, marié, etc.), (11) numéro de CIN, (12) numéro d'acte de naissance, (13) lieu de naissance, (14) nationalité.</p>
Données biométriques	Aucun
Déduplication	Via les 8 critères indiqués ci-dessus (uniquement démographiques)
Type d'identification	Numéro d'identification seulement, aucune carte ou autre justificatif d'identité émis
Format numérique	10 chiffres : 8 numéros séquentiels (anonymes) plus 2 chiffres de contrôle
Architecture de base de données	Base de données centralisée
Bases de données avec lesquelles le système échange des informations	CNRPS (quotidien) CNSS (quotidien) MAS (une fois tous les trois mois)
Technologie de base de données	Oracle 12c, 8 Go
Sauvegarde et reprise après sinistre	Sauvegarde complète quotidienne avec Backup Exex 2014, pas de site de secours

Depuis le début de sa mise en œuvre, l'intégration entre l'IS et les programmes sociaux a considérablement progressé, dans le cadre de la coopération entre le MAS, le CRES, la CNSS, la CNRPS et la CNAM. Le Tableau 15 résume ces avancées avec des informations de base sur ces trois programmes principaux.

Tableau 15 . Récapitulatif de l'identification pour les principaux systèmes de protection sociale

	MAS	CNSS	CNRPS	CNAM
Qui est couvert	Les bénéficiaires du programme d'assistance à la sécurité (PNAFN et AMG1 / 2)	Employés du secteur privé et les personnes à leur charge	Les employés du secteur public et les personnes à leur charge	Les employés assurés par la CNRPS et la CNSS et les personnes à leur charge
Couverture cible	2,3 millions	~ 9,6 millions	~ 1,8 million	~ 8,5 millions
Couverture IS	1 million (53%) ^a	8,1 millions (84%)	1,7 million (95%)	5.8 millions (83.5%) ^b
Données biographiques	Prévu : en conformité avec les nouvelles cartes CNAM	Données d'identification (8 critères) : prénom, nom de famille, prénom du père, prénom du grand-père, prénom de la mère, nom de famille de la mère, date de naissance et sexe Informations sur le programme : par exemple, régime, lieu de naissance, personnes à charge, salaire Identifiants supplémentaires : numéro d'acte de naissance, numéro de CIN et date de délivrance	Données d'identification (8 critères) : prénom, nom de famille, prénom du père, prénom du grand-père, prénom de la mère, nom de famille de la mère, date de naissance et sexe Informations sur le programme : par exemple, personnes à charge, etc.	Prévu : en conformité avec les nouvelles cartes CNAM
Biométrie	Aucun	Aucun	Aucun	Aucun
Déduplication	Via l'IS	Déduplication démographique avant génération du numéro CNSS	Via l'IS	Via l'IS
Justificatif (identifiants)	Prévu : extension de la carte CNAM aux bénéficiaires du MAS	Seul numéro CNSS émis spécifique au bureau régional où il a été inscrit, 10 chiffres : 1 code d'activité Racine à 7 chiffres 1 code de compte 1 chiffre de contrôle	Seul le numéro CNRPS est émis	Prévu : Carte CNAM (code à barres 2D)

	MAS	CNSS	CNRPS	CNAM
Intégration de l'IS	Les personnes nouvellement inscrites sont envoyées au CRES, car elles sont enregistrées dans la nouvelle base de données du MAS (fréquence non déterminée)	Tous les jours, les nouveaux inscrits et les mises à jour à la CNSS sont envoyés au CRES via un serveur FTP	Les nouveaux candidats sont vérifiés par rapport à la base de données du CRES pour récupérer / attribuer un IS. Les données sont envoyées via une requête de serveur FTP au CRES plusieurs fois par jour	La CNAM utilise le IS comme données obligatoire pour s'inscrire à toutes les prestations de l'assurance maladie. Ainsi, tout bénéficiaire sans IS est systématiquement redirigé à la caisse d'affiliation pour l'attribution de l'IS ou la correction de données.
Intégration avec d'autres bases de données	CNSS CNRPS <i>Madania</i>	CNAM : La CNSS envoie des données à la CNAM toutes les deux semaines pour mettre à jour les enregistrements du système d'information et les erreurs (via la base de données Oracle), et deux fois par semaine (via un serveur FTP) avec les nouvelles inscriptions. Madania : la CNSS envoie des demandes de lot pour vérifier les informations de naissance via le numéro du certificat de naissance.	CNAM : la CNRPS envoie des données à la CNAM, y compris des vidages de données mensuels avec des informations sur la retraite et des mises à jour quotidiennes (via un serveur FTP) sur les personnes nouvellement assurées. Madania : la CNRPS envoie des requêtes à la demande pour vérifier les informations de naissance via les 8 critères.	Ministère de la santé : factures Banques / poste : données sur les transferts Ministère des finances : données sur les prestataires de soins Madania (processus non vérifié)

Source : TALYS Consulting, 2019 Rapport d'audit IS.

- a. Parmi les bénéficiaires du programme d'assistance sociale, environ 30% des membres se trouvent dans la base de données de la sécurité sociale lors du recoupement avec l'IS.
- b. Actuellement, il y a des enfants et des conjoints qui figurent dans la base de données de la CNAM mais pas dans la base de données de la sécurité sociale et ils tentent de résoudre ce problème car le droit à l'assurance maladie découle de la cotisation à la sécurité sociale.

Les sections ci-dessous décrivent l'intégration du système d'information dans des bases de données distinctes sur la protection sociale, ainsi que les défis persistants.

La base de données du MAS pour les programmes d'assistance sociale (système non contributif)

L'intégration de l'IS dans la base de données du MAS a débuté en 2016 avec la volonté de développer le registre des bénéficiaires des programmes d'assistance sociale, notamment le PNAFN et l'AMG1 / 2. Jusqu'ici, sur un total d'environ 2,3 millions de bénéficiaires (appartenant à 0,9 million des ménages), quelques 1,3 millions de personnes ont été saisies dans le nouveau système de gestion de l'information du MAS. Cependant, l'IS a été attribué à environ 1 million. Cet écart a deux causes : premièrement, des retards / des irrégularités dans l'envoi des données du MAS au CRES afin d'attribuer l'IS. Deuxièmement, sur les données reçues par le CRES, 20% ont été rejetées en raison d'un manque d'informations principales nécessaires à la génération de l'IS. La couverture IS devrait augmenter à mesure que le MAS collectera et enverra plus de données au CRES et que les cas rejetés sont corrigés.

À la suite de l'attribution de l'IS, environ 30% des membres de la famille des bénéficiaires du programme d'assistance sociale ont été retrouvés dans la base de données de la sécurité sociale (c'est-à-dire les bases de données CNSS et CNRPS). Cela signifie que l'IS facilitera grandement la capacité du MAS à vérifier les données administratives relatives au bien-être des bénéficiaires potentiels et actuels. Plus précisément, le MAS aura une plus grande capacité d'évaluation et de réévaluation des besoins et de l'éligibilité des bénéficiaires du programme de protection sociale, sur la base du statut de contribution à la sécurité sociale de tous les membres de la famille. Actuellement, les travailleurs sociaux contrôlent manuellement la base de données de la CNSS pour vérifier les cotisations de sécurité sociale des membres individuels des ménages bénéficiaires. Ce processus devrait devenir plus rapide et plus efficace grâce à une nouvelle plateforme d'échange de données et à un nouveau mécanisme de ciblage.²⁷ Cela intégrerait des informations relatives à la CNSS et à la CNRPS, qui peuvent être vérifiées automatiquement à l'aide de l'IS, pour la communication entre bases de données.

Caisses de sécurité sociale (systèmes contributifs, CNSS et CNRPS)

Les employés du secteur privé s'inscrivent à la CNSS dans l'un des 49 bureaux régionaux et locaux en fournissant notamment leur acte de naissance, les actes de naissance des personnes à leur charge et leur CIN. Comme pour la CNRPS, huit critères sont ensuite collectés : prénom, nom de famille, prénom du père, prénom du grand-père, prénom de la mère, nom de famille de la mère, date de naissance et sexe. L'identité du demandeur est ensuite vérifiée et une recherche dans la base de données de la CNSS est effectuée pour déterminer si une personne de même sexe, nom et date de naissance s'est déjà inscrite. Si le demandeur ne figure pas dans la base de données, ses critères sont enregistrés et un numéro de CNSS lui est attribué à partir de la banque de numéros réservés au bureau. Étant donné que le nombre change lorsque les personnes changent de régime, le bénéficiaire ne garde pas un numéro unique à travers le temps et la probabilité que deux personnes aient le même numéro CNSS est d'environ un cas sur 40 000. Systématiquement, la CNSS envoie la demande de création de l'IS pour les nouvelles immatriculations ainsi que les mises à jour concernant le changement de régime, de position ou de situation ainsi que toute correction de l'identité des bénéficiaires.

Pour s'inscrire à la CNRPS, les travailleurs du secteur public - par l'intermédiaire de leur employeur (un ministère ou une entreprise publique) - doivent fournir des pièces justificatives, notamment leur acte de naissance (en arabe), leur CIN et un certificat de travail dans l'un des 24 centres d'enregistrement régionaux et / ou sept centres locaux. L'identité du demandeur est vérifiée à l'aide de huit critères (en arabe) : prénom, nom de famille, prénom du père, prénom du grand-père, prénom de la mère, nom de famille de la mère, date de naissance et sexe. Ces données sont d'abord envoyées à la base de données centrale CNRPS, qui envoie ensuite les huit critères de certification au CRES. Ensuite, le CRES renvoie (a) le numéro IS de la personne, s'il en a un déjà généré, ou (b) attribue un nouveau numéro IS, qui est ensuite enregistré dans la base de données CNRPS. La CNRPS vérifie également les informations d'enregistrement des naissances en envoyant des requêtes numériques au REC *Madania* qui utilise les mêmes huit critères. Les règles de gestion imposent un délai de traitement de 48 heures pour l'attribution de l'IS, après l'envoi de la demande par l'employeur.

Malgré les progrès réalisés, l'intégration de l'IS dans les systèmes CNSS et CNRPS pose encore quelques problèmes :

- Absence des huit critères nécessaires pour émettre l'IS (environ 2% pour le CNRPS).
- Un écart de données entre les fonds de sécurité sociale (CNSS et CNRPS) et le CRES est possible (par exemple, le CNSS n'envoie pas directement les mises à jour au CRES, il n'existe pas actuellement de règles de gestion pour envoyer un IS à la base de données de la CNSS).

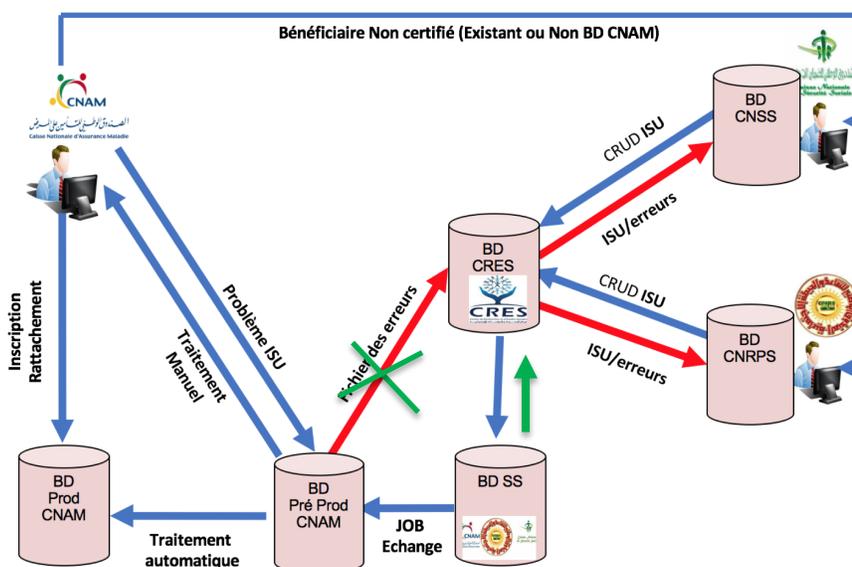
²⁷ En outre, un nouvel outil de ciblage fournira des informations supplémentaires sur le bien-être des ménages en utilisant des critères objectifs et une procédure transparente. Un test des moyens de substitution (PMT) est actuellement en cours de développement sur la base de l'enquête officielle de l'INS, tandis qu'un test des moyens hybrides consistera également à explorer les données administratives liées au revenu.

- Tous les membres de la famille ne sont pas toujours déclarés aux fonds de la sécurité sociale. Cela est principalement dû à la pratique d'inscription à la CNAM selon laquelle les informations sur les conjoints, les enfants ou les personnes à charge sont souvent mises à jour uniquement par la CNAM, bien que leur droit à l'assurance-maladie découle de leur contribution à la CNSS / CNRPS. En conséquence, les informations sur les membres de la famille ne sont souvent pas entièrement mises à jour dans les bases de données CNSS / CNRPS et un IS n'est pas délivré à tous les membres de la famille. (Par exemple, seulement 30% des familles présentent des informations similaires concernant les clusters familiaux dans les bases de données de la CNAM et du CRES en 2018).²⁸
- Le système d'information de la CNSS reste partitionné et composé de plusieurs applications indépendantes utilisant l'identification interne (numéro CNSS), et non l'IS.
- L'échange de données entre la CNSS et la CNAM est basé sur le numéro du CNSS et non sur l'IS.
- Après le décès d'un retraité, les membres survivants de la famille reçoivent leur pension par le biais du numéro IS du défunt (avec un préfixe). Ils ne sont donc pas eux-mêmes identifiés à un IS dans le système d'information de la gestion de la pension. (L'IS est octroyé à travers l'application d'immatriculation des assurés sociaux pour qu'ils puissent bénéficier d'une assurance maladie).

Caisse d'assurance maladie (CNAM)

Auparavant, la base de données du CNAM était alimentée par la CNRPS et la CNSS, qui envoient des enregistrements périodiques de leurs bénéficiaires, qui sont automatiquement couverts par la CNAM. En tant que tels, les nouveaux inscrits à la CNAM devraient avoir les IS (ou bien des numéros CNSS) qu'ils ont reçus lors de leur inscription auprès de l'une des deux caisses de sécurité sociale. Toutefois, vue l'urgence de fournir les prestations de l'assurance maladie, la CNAM pendant un certain temps a procédé à l'inscription et a offert des prestations aux membres de la famille (conjoints et enfants) non enregistrés à la CNSS ou à la CNRPS et qui ne possédaient pas encore d'IS. Afin de résoudre ce problème, les inscriptions ont été arrêtées en 2014 et à nouveau en 2016, après avoir recommandé d'organiser une campagne médiatique pour faire en sorte que les membres de la famille de l'assuré obtiennent d'abord un IS. Il s'agit de leur demander de s'inscrire au préalable auprès de la CNRPS ou de la CNSS et d'obtenir un IS, avant de s'inscrire à la CNAM (voir Schéma 12).

Schéma 12 . Processus de vérification des bénéficiaires de la CNAM



Source : Présentation du CNAM sur les IS

28 TALYS Consulting. 2019 Rapport d'audit IS.

Cependant, le système d'information n'est actuellement pas utilisé par la CNAM. Les problèmes spécifiques liés à l'intégration comprennent notamment :

- Les données relatives à la CNAM sont collectées et entrées en français (plutôt qu'en arabe) et n'incluent pas les huit critères nécessaires à la vérification.
- Il existe des erreurs de saisie de données, notamment au niveau de l'identité (date de naissance, nom de famille) et des numéros de la CIN.

Projets de cartes de santé / protection sociale et d'authentification (cartes CNAM)

Actuellement, les patients ont accès aux prestations d'assurance maladie en utilisant une carte d'identité papier et le processus de réclamation entre les bénéficiaires, les prestataires de soins de santé et la CNAM est essentiellement manuel. Au milieu de 2018, la CNAM a lancé un projet visant à moderniser l'administration du fonds, à réduire les coûts globaux, à permettre un transfert direct de données entre les prestataires de soins de santé et la CNAM et à améliorer la qualité des services fournis aux citoyens. Le projet comprend trois composantes, à savoir : 1) la mise en place d'un système d'échange de données informatisé (SEED) entre le fonds et les prestataires de soins de santé, 2) l'amélioration de la gestion de l'accès à l'identité et de la sécurité, et 3) la délivrance d'une nouvelle carte remplaçant la carte papier actuelle.²⁹

Malgré les plans antérieurs pour une carte à puce, la CNAM a décidé de mettre en œuvre une carte basique avec un code à barres 2D pour stocker les données cryptées, y compris le numéro IS, permettant l'authentification via la plate-forme CNAM. Cette carte renforcera la gouvernance de l'assurance maladie grâce à une meilleure identification des personnes lors de l'accès aux services de santé. Du fait que l'assurance maladie est gérée au niveau des ménages, une seule carte sera initialement émise par famille, tandis qu'un plan futur inclut l'émission de cartes supplémentaires à d'autres membres éligibles du ménage. La distribution de ces nouvelles cartes aux bénéficiaires de la CNAM - le programme d'assurance maladie ordinaire contributive - a débuté en avril 2019.

Basée sur la même solution/technologie de la carte CNAM, le MAS a commencé aussi à distribuer des cartes aux bénéficiaires de l'assistance sociale du MAS du programme d'assurance maladie pour les nécessiteux, lesquelles pourraient être la même que la carte CNAM dans le futur (pour ne pas distinguer les bénéficiaires du système contributifs et non contributifs), élargie aux membres du ménage (pas uniquement au chef de ménage) et y intégrer une photo d'identité. En utilisant la même solution d'identification pour tous les programmes, les nouvelles cartes de santé / protection sociale permettront à l'administration de mieux gérer les cas des personnes qui changent de statut entre les programmes destinés aux nécessiteux et les programmes réguliers (systèmes non contributifs et contributifs)³⁰ via un système back-end plutôt que d'indiquer leur statut de manière visible sur les cartes. Cela aidera également à protéger la vie privée et à réduire la stigmatisation sociale potentielle vécue par les bénéficiaires des programmes pour indigents. Une fois que les cartes auront été délivrées à la population cible de bénéficiaires, environ 90% de la population tunisienne disposera d'un moyen plus commode et plus sûr pour s'authentifier lorsqu'ils accéderont aux services de santé.

29 Depuis près de 10 ans, MAS envisageait de lancer une carte plus évoluée pour les bénéficiaires d'assurance maladie. Toutefois, trois précédentes séries de passations de marchés ont été infructueuses : lance-la-smart-carte-au-profit-de-ses-affiliés /

30 À long terme, ces cartes basiques pourraient être remplacées par des solutions plus sophistiquées lorsqu'elles deviendraient disponibles dans le cadre de projets nationaux de cartes d'authentification / cartes d'identité électroniques.

Voies à suivre

Sur la base des conclusions de l'audit de l'IS, le CRES a préparé une feuille de route pour continuer à améliorer l'IS.³¹ Le plan d'action comprend notamment : (i) la synchronisation de l'IS avec différentes données, en particulier ceux de *Madania*, via un service web ; l'amélioration de la gestion des dictionnaires (définition de l'accès, spécification du flux de travail, harmonisation des dictionnaires (ex: prénom et nom)); (ii) mise en place d'une nouvelle plate-forme permettant de suivre les problèmes liés à la qualité des données (cela permettra de définir le protocole d'échange de données, les utilisateurs, les règles de contrôle des données); (iii) la spécification des modalités permettant d'améliorer la fiabilité des données (par exemple, le recoupement automatique des identités avec *Madania*, pour les flux de données stockées et nouveaux, la détection des doublons); et (iv) la refonte du processus d'attribution et de modification de l'IS pour différentes parties prenantes, y compris la structure d'organisation et de gouvernance.

Le secteur de la santé

Les hôpitaux publics de niveaux 2 et 3 (c'est-à-dire les hôpitaux régionaux et les centres hospitaliers universitaires) ont actuellement chacun leur propre système d'information indépendant permettant d'identifier les patients localement. Ces numéros d'identification au niveau de l'hôpital sont composés de dix chiffres et incluent l'année d'enregistrement de la personne et un numéro séquentiel à six chiffres par établissement qui redémarre à zéro chaque année. En plus du nom du patient, du sexe, de la date de naissance, du gouvernorat de naissance, de l'état matrimonial et des prénoms de la mère et du père, les systèmes d'information hospitaliers enregistrent également le numéro de la CIN de la personne et le numéro de la carte CNAM. Cependant, ces informations ne sont pas systématiquement capturées et il existe un risque d'attribution d'une identification différente pour le même patient lors de visites médicales différentes.

Bien que ces identifiants créent un enregistrement pour les patients d'un établissement donné, ces systèmes ne sont ni centralisés ni interopérables, ce qui signifie qu'une personne doit s'inscrire à nouveau dans chaque établissement et sera saisie dans plusieurs établissements portant plusieurs numéros. De plus, il n'y a pas d'interopérabilité entre les prestataires de santé publics et privés, ce qui pose problème, car de nombreux patients utilisent plusieurs établissements, de type public ou privé. En conséquence, les patients ne disposent pas de dossiers de santé électroniques complets et portables, et les hôpitaux n'ont pas une vision unifiée de leurs antécédents.

Le Ministère de la santé mène actuellement une étude de planification visant à améliorer les systèmes d'information et d'identification des patients dans les hôpitaux. Bien qu'il existe déjà un accord préliminaire sur l'intégration dans ce système de l'IS, il est également possible que ce système puisse utiliser l'IUC à l'avenir (en veillant à respecter les principes de non-prolifération de cet ID dans les bases sectorielles en utilisant les mécanismes de tokenization), par exemple pour couvrir le faible pourcentage de la population qui n'aura pas de système d'assurance³².

31 Voir Talys Consulting et CRES. "CRES - Feuille de route des projets." (Présentation).

32 Environ 90% de la population tunisienne devrait être couverte par des régimes d'assurance maladie contributifs et non contributifs et aura donc reçu un IS.

Éducation

Le Ministère de l'Éducation dispose de systèmes d'information permettant de gérer les données relatives aux élèves des écoles primaires et secondaires dans les établissements publics. Auparavant, les numéros attribués aux établissements n'étaient pas centralisés ni interopérables, ce qui signifie qu'un nouveau numéro était attribué à chaque élève chaque fois qu'il déménageait dans une école sans lien permettant de maintenir la continuité des dossiers des élèves. A partir de 2018, le ministère de l'Éducation a collaboré avec le MTCEN et le MALE pour simplifier le processus d'inscription des élèves du secondaire en utilisant le système *Madania*. En 2019, les parents ont préenregistré leurs enfants à l'école primaire en ligne et n'ont plus besoin de présenter d'acte de naissance, grâce au système e-madhmoun décrit précédemment. Cela a été étendu pour couvrir les inscriptions dans les écoles secondaires et couvrira également les écoles privées au cours d'une phase ultérieure. Dans le nouveau système les élèves sont identifiés par un numéro unique généré après avoir vérifié son existence dans l'état civil et suite à la création de mapping entre cet identifiant fonctionnel et l'IUC. En 2019, cet identifiant sectoriel couvre environ 2 millions d'élèves. Il faut que le Ministère de l'Education assure que toute nouvelle inscription passe par ce processus surtout pendant la scolarité.

Les taxes

Au sein du ministère des finances, la direction générale des impôts détient une base de données des contribuables et délivre un numéro d'identification fiscale : *le matricule fiscal*. En 2015, environ 3 millions de personnes étaient inscrites dans le système, dont 566 000 environ sont identifiées par leur numéro d'identification fiscale et sont des contribuables actifs. Pour s'inscrire dans le système, les contribuables doivent fournir leur numéro de CIN, ainsi que leurs nom, date de naissance, adresse et profession. La direction reçoit également des informations des employeurs (et de la CNSS via l'INS), du Ministère de l'Intérieur (concernant les infractions au code de la route) et du ministère du Travail (concernant d'autres infractions).

4. Cadre juridique

La Tunisie dispose d'un cadre juridique relativement complet pour ses systèmes d'identification, y compris des décrets et des lois organiques qui habilitent les agences d'identification et d'enregistrement des faits d'état civil, régissent le traitement – la collecte, le stockage, l'utilisation, le transfert, etc. - des données à caractère personnel, contiennent des dispositions concernant la protection des données et établissent un organisme indépendant chargé de superviser le traitement des données conformément à cette loi (c'est-à-dire l'INPDP). Ce cadre juridique a été passé en revue dans le rapport de 2015 commandé par le MTCEN et, par conséquent, le catalogage détaillé des lois tunisiennes relatives à l'identité n'est pas au centre du présent rapport. Cependant, cette section fournit un bref aperçu du projet de LPDP et du projet de code numérique, qui sont, à des stades différents, examinés actuellement par l'Assemblée nationale tunisienne. Chacune de ces lois est essentielle à la mise en œuvre et à la gestion des identifiants IUC, IS et autres, ainsi que des services d'identité et de la confiance numérique au sens large.³³

Projet de loi organique sur la protection des données à caractère personnel (LPDP)

Comme décrit ci-dessus, L'Assemblée nationale tunisienne étudie actuellement un projet de loi sur la protection des données (LPDP) qui définit certains éléments de base de la conception de l'IUC (voir Encadré 3). En outre, cette loi s'appliquera plus largement à toutes les entités - publiques et privées - qui traitent des données à caractère personnel sur le territoire tunisien, y compris les bases de données de base et celles fonctionnelles décrites ci-dessus (LPDP Article 2). Elle vise à actualiser la loi de 2004 sur la protection des données afin de clarifier certains domaines ambigus ³⁴ et de l'harmoniser avec la nouvelle constitution de 2014 et avec les principes internationaux relatifs à la vie privée et à la protection des données, tels que le RGPD et la Convention 108+ du Conseil européen, auxquels la Tunisie a adhéré en 2017.³⁵ Le projet de LPDP a été approuvé par le conseil des ministres en mars 2018 et est en discussion à l'Assemblée nationale depuis 2018.

Le projet de loi spécifie notamment les droits, principes et réglementations suivants, en matière de traitement de données :³⁶

- **Droit à la vie privée et à la protection des données :** Le droit à la protection des données (article 1), qui complète le droit à la vie privée consacré à l'article 24 de la constitution tunisienne de 2014.
- **Supervision :** Le traitement des données sera supervisé par une autorité publique indépendante (article 1) qui autorisera le traitement des données à caractère personnel (article 9). Cette autorité est l'INPDP, créée par décret en 2007.³⁷

33 ID4D a mis au point un outil supplémentaire permettant de procéder à une analyse plus approfondie du cadre juridique de l'ID, appelé l'Evaluation de l'Environnement Favorisant l'Identification (ID Enabling Environment Assessment - IDEEA). La version actuelle des directives IDEEA est disponible à l'adresse suivante : <http://id4d.worldbank.org/legal-assessment>.

34 La loi remplacera ou complètera le cadre juridique existant sur ce sujet, y compris la loi organique 2004-63 sur la protection des données à caractère personnel, qui peut être trouvée avec d'autres textes pertinents ici : <http://www.inpdp.nat.tn/textes.xhtml>.

35 Voir https://www.coe.int/fr/web/data-protection/home/-/asset_publisher/RMbj8Pk1ApgJ/content/welcome-tunisia-new-party-to-convention-108.

36 Les traductions sont effectuées par les auteurs et ne sont pas officielles. Consultez le projet de loi en français et en arabe pour obtenir le texte complet et précis. Les numéros d'article de cette section proviennent de la version 2017 du projet de loi en français ; ils peuvent différer de ceux en cours de discussion au Parlement, dont le texte est en arabe.

37 Pour le texte intégral du décret n ° 2007-3003 en français et en arabe, voir : http://www.inpdp.nat.tn/ressources/decret_3003.pdf. Les procédures d'autorisation du traitement des données à caractère personnel par l'INPDP peuvent également être trouvées dans le décret n ° 2007-3004 au : http://www.inpdp.nat.tn/ressources/decret_3004.pdf.

- **Transparence** : Le traitement doit être connu du public et approuvé par l'INPDP, qui tiendra un registre des processeurs de données autorisés sur son site Web (article 5). Les personnes concernées ont également le droit d'être informées de l'existence d'un processus de décision automatisé basé sur leurs données (article 6).
- **Respecter et ne pas nuire** : Les données à caractère personnel doivent être traitées de manière loyale et transparente, et le traitement des données personnelles doit se faire dans le respect de la dignité humaine, de la vie privée et des libertés publiques et individuelles et ne doit en aucun cas porter atteinte aux droits des personnes, leur nuire ou nuire à leur réputation (article 8).
- **Minimisation** : Le traitement des données doit être adéquat, pertinent et non excessif au regard des finalités pour lesquelles elles ont été collectées (article 8).
- **Limite de stockage et droit à l'oubli** : Les données ne peuvent être stockées que sous une forme permettant l'identification des personnes concernées pendant une période n'excédant pas celle requise aux fins pour lesquelles elles sont traitées (article 8). Une fois que l'objectif du traitement des données a été atteint, les responsables du traitement doivent détruire ou rendre anonymes ces données (article 64).
- **Qualité et précision** : Le responsable du traitement doit s'assurer que les données sont exactes et à jour (article 8). Le responsable du traitement et le responsable du traitement doivent corriger, ajouter, modifier ou mettre à jour les données personnelles et les supprimer si elles se rendent compte de leur inexactitude ou de leur insuffisance ou si l'objectif pour lequel elles ont été collectées est atteint (article 17).
- **Spécification de but** : La collecte de données à caractère personnel ne peut être effectuée qu'à des fins licites, déterminées, explicites et déclarées. Le traitement de données à caractère personnel ne peut être effectué à des fins autres que celles pour lesquelles il a été collecté que si la personne concernée a donné son consentement ou si le traitement est nécessaire pour sauvegarder un intérêt vital de la personne concernée (article 9).
- **Données sensibles** : Le traitement de données à caractère personnel révélant directement ou indirectement l'origine raciale, ethnique ou génétique, les données biométriques, l'emplacement, les convictions religieuses, les opinions et affiliations politiques, philosophiques et syndicalistes, les données relatives à la santé, la vie sexuelle ou à l'orientation sexuelle d'une personne physique est interdite sauf si elle est effectuée avec le consentement exprès de la personne concernée sur la base d'informations adéquates, ou si un tel traitement est nécessaire pour sauvegarder les intérêts vitaux de la personne concernée conformément aux règles définies par cette loi. Le traitement de données à caractère personnel liées à des infractions, aux poursuites et enquêtes s'y afférant, à des sanctions, à des mesures préventives ou à un casier judiciaire n'est autorisé que par les tribunaux et les assistants juridiques, dans les limites et dans les conditions fixées par le tribunal. (Article 11).
- **Interdiction de lier un avantage à un consentement** : Il est strictement interdit de lier la fourniture d'un service ou l'octroi d'un avantage à une personne à l'acceptation du traitement de ses données à caractère personnel ou de l'exploitation de ses données à des fins autres que celles pour lesquelles elles ont été collectées (article 12).
- **Sécurité des données** : Toute personne qui, personnellement ou par l'intermédiaire d'un sous-traitant, gère le traitement des données à caractère personnel doit prendre toutes les précautions nécessaires pour assurer la sécurité de ces données et empêcher les tiers de les modifier ou de les consulter sans le consentement de la personne concernée. (Article 13). Les informations relatives aux atteintes à la sécurité doivent être signalées à l'INPDP dans les 48 heures et aux personnes concernées dans les meilleurs délais (article 14).
- **Consentement éclairé** : Le traitement des données à caractère personnel ne peut être effectué qu'avec le consentement de la personne concernée ; il doit être libre, spécifié, informé, sans ambiguïté, explicite et doit laisser une trace écrite ou électronique (article 38). Il peut être retiré à tout moment (article 39).

- **Droit d'accès** : Permettre à la personne concernée d'accéder sans retard, à des intervalles raisonnables, à ses données à caractère personnel, d'en obtenir une copie et de demander que lui soient apportées des corrections ou bien qu'elles soient supprimées (article 47).
- **Transferts de données vers d'autres pays** : Le transfert de données à caractère personnel vers un autre pays n'est autorisé que si ce pays offre un niveau de protection équivalent et nécessite l'autorisation de l'INPDP. Le transfert de données vers d'autres pays est interdit lorsque cela risque de compromettre la sécurité publique ou les intérêts vitaux de la Tunisie (articles 35 et 36). Les données à caractère personnel traitées par des entreprises publiques ne peuvent pas être hébergées en dehors du territoire national (article 132).
- **Exceptions à la loi** : Conformément à l'article 49 de la Constitution, la loi prévoit deux exceptions : 1) la sécurité nationale ou publique, les intérêts financiers ou économiques importants de l'État, l'impartialité et l'indépendance du pouvoir judiciaire, et / ou la prévention, l'instruction ou les poursuites d'infractions pénales, ou (2) la protection de la personne concernée ou des droits et libertés fondamentaux d'autrui, y compris la liberté d'expression (article 4).

En outre, le LPDP confirme les responsabilités de l'INPDP - défini comme un organe indépendant, financièrement autonome et légalement constitué (article 140) - qui comprennent, sans s'y limiter : l'habilitation des responsables et l'autorisation des processus de traitement des données ; la réception des plaintes et le traitement des différends relevant de sa compétence ; l'élaboration des règles et des directives pour le traitement des données personnelles ; la garantie du respect des normes légales et réglementaires ; la collaboration avec l'autorité nationale pour l'accès à l'information et d'autres institutions de réglementation pour prendre des décisions et établir des lignes directrices sur l'accès aux données et la réalisation d'évaluations périodiques concernant le respect des lois sur la protection des données (article 141).

Code numérique

Le gouvernement a mis au point un nouveau Code Numérique destiné à stimuler et à réglementer le développement d'une économie numérique, actuellement en phase de consultation publique. En plus d'encourager la concurrence et les investissements dans les communications et le commerce numériques et de renforcer la confiance dans les transactions numériques, la loi a pour objectif spécifique de réduire la fracture numérique dans l'ensemble du pays et de répondre aux besoins des particuliers et des institutions. Bien que le Code ne traite pas spécifiquement des systèmes d'identité, il contient des dispositions régissant les services de confiance numérique, y compris les signatures et certificats électroniques et les services de cryptage, qui sont utilisés pour l'authentification et l'autorisation numériques des services et transactions électroniques.

Les éléments pertinents du code comprennent, sans s'y limiter :³⁸

- **Les documents électroniques** : Définis comme des documents composés d'un ensemble de lettres, de chiffres ou d'autres signaux numériques - y compris ceux échangés par un moyen de communication - dont le contenu peut être compris et stocké sur un support électronique et peut être lu et référencé en cas de besoin (article 149). Les documents électroniques sont considérés comme des instruments officiels s'ils sont accompagnés d'une signature numérique fiable (article 151). Dans tous les cas où des dispositions législatives ou ordinales exigent la conservation de documents papier, cette exigence est remplie par le biais d'un service d'archivage électronique. En outre, la version électronique d'un document papier est considérée comme une copie originale et valide à long terme lorsqu'elle est créée et enregistrée à l'aide d'un

³⁸ Cette analyse repose sur une traduction non officielle et non vérifiée du projet du code numérique en version arabe par les auteurs.

service capable de l'archivage électronique. Dans ce cas, le document papier original peut être détruit, sauf dispositions légales en vigueur contraires (articles 181 à 184, voir aussi article 266).

- **Signatures numériques** : Les signatures numériques seront acceptées à la place des signatures écrites et seront valides devant les tribunaux, sauf preuve de leur manque de fiabilité (articles 152, 160 à 161). Si les documents sont signés électroniquement, une méthode d'identification fiable doit être utilisée pour s'assurer que la signature est liée au document électronique qui lui est associé (article 149, voir aussi l'article 154-156 pour plus d'informations sur les conditions de fiabilité).
- **Vérification d'identité pour les fournisseurs de confiance numérique** : Avant de délivrer des certificats, les fournisseurs de services de confiance numérique doivent collecter des informations personnellement identifiables via une procédure de contact personnel, sur la base d'un certificat de signature électronique authentique et valide délivré par le même fournisseur ou un autre fournisseur agréé (article 167).
- **Sécurité et supervision des données** : Les systèmes d'information et les réseaux d'agences publiques doivent faire l'objet d'audits de sécurité numériques obligatoires et périodiques, effectués par l'Agence Nationale de la Sécurité Numérique, à l'exception des Ministères de la Défense Nationale, de l'Intérieur et du Développement local (c'est-à-dire le MALE), auxquels l'Agence nationale de la sécurité numérique invitera à mener un audit interne (articles 209 et 210).
- **Principe unique** : Les entités publiques ne doivent pas demander à quelqu'un de fournir des données pouvant être obtenues à distance auprès d'autres entités publiques. Toutes les données publiques et personnelles échangées entre des structures publiques sont identiques à l'authenticité juridique des documents papier. Dans les cas où le déposant doit envoyer ou déposer plusieurs exemplaires d'un même document, cette condition est considérée comme remplie dans le cas d'un document électronique une fois qu'un exemplaire unique du document a été envoyé ou déposé (article 270).
- **Interopérabilité** : Les entités publiques adoptent les règles techniques nécessaires pour assurer l'échange de données et de documents sans compromettre leur intégrité ou l'accès qui y est dû (article 275).

PARTIE 3. Construire un écosystème d'identité numérique pour la Tunisie : Opportunités, défis et recommandations

Le gouvernement tunisien s'est fermement engagé à améliorer l'identification des citoyens dans le cadre d'une stratégie plus large de transformation numérique dans le cadre du PNS. Comme le montre la partie 2 du présent rapport, le gouvernement a réalisé des progrès significatifs à cet égard et la Tunisie a le potentiel de devenir un leader régional en matière d'identification. En même temps, un certain nombre de lacunes et de défis subsistent. Cette section résume les principaux points forts, opportunités, faiblesses et risques des projets en cours liés à l'identification, puis fait une série de recommandations afin d'aider le gouvernement à mieux exploiter son élan et de faire en sorte que ses systèmes d'identification répondent aux objectifs du gouvernement et du peuple tunisien.

1. Points forts et opportunités

Systemes d'identification de base avec une couverture élevée

La Tunisie a réussi à mettre en place de solides systèmes d'identification de base — notamment le REC et la CIN - qui fournissent une preuve d'identité de base pour presque toute la population. Ce n'est pas un mince exploit et signifie que la Tunisie est en voie d'atteindre la cible 16.9 de l'Objectif de Développement Durable (ODD), qui consiste à « fournir une identité juridique à tous, y compris l'enregistrement des naissances » d'ici 2030. Outre la couverture, l'adoption d'un système informatisé d'enregistrement de l'état civil (*Madania*) a considérablement amélioré l'accessibilité des certificats du REC à la population, accéléré le traitement des statistiques de l'état civil, rationalisé de nombreuses procédures administratives dans les municipalités et limité les services de vérification de l'identité fournis à d'autres entités publiques.

Un engagement à construire une infrastructure d'identité numérique

Comme indiqué ci-dessus, le GT met actuellement en œuvre ou planifie **plusieurs projets liés à l'identité numérique** dans le cadre ou en relation avec le PNS, y compris l'IUC, l'IS, le registre social, la mise à niveau de *Madania*, la carte eCIN potentielle, la plate-forme d'interopérabilité TunXRoad, l'authentification numérique et les signatures électroniques par TUNTRUST, la mise à niveau des systèmes d'informations sanitaires et la carte à puce CNAM. De nombreux autres projets du PNS, tels que les portails gouvernementaux en ligne et les services électroniques, s'appuieront sur ces systèmes pour l'interopérabilité, l'authentification numérique, etc. L'implication de multiples parties prenantes et des ressources importantes dans ces projets démontrent un engagement significatif - et une demande pour - le développement d'un écosystème d'identité robuste et d'une forte capacité technique des ministères.

Le système IUC intègre des conceptions favorables à la confidentialité et au contrôle de l'utilisateur

Selon les prévisions actuelles, l'IUC sera un numéro de back-end uniquement qui ne peut pas être stocké dans d'autres bases de données ni rendu public. **Cette conception - qui est articulée dans le nouveau LPDP - est intentionnellement destinée à protéger la confidentialité des données** en réduisant la prolifération d'un identifiant unique sur plusieurs systèmes, ce qui peut créer certains risques pour la protection des données. Au lieu de cela, l'IUC facilitera la vérification de l'identité et l'interopérabilité en enregistrant un mappage de l'IUC avec d'autres identifiants sectoriels dans le système central uniquement.³⁹ En outre, la plate-forme IUC comprendra un **portail permettant aux utilisateurs d'accéder à leurs données et de les consulter**, renforçant ainsi la surveillance individuelle. Si ces conceptions sont bien mises en œuvre - avec d'autres mesures de protection de la vie privée et de sécurité - le modèle tunisien pourrait fournir un exemple nouveau et innovant à suivre pour les autres pays.

Des progrès significatifs concernant les systèmes IUC, REC et ceux de protection sociale

Conformément aux objectifs du PNS, le GT a fait **des progrès significatifs dans un certain nombre de domaines prioritaires** qui concernent notamment les systèmes d'identification de base, la conception et le début de la mise en œuvre de l'IUC et la spécification et la définition détaillée d'un plan de mise en œuvre visant à réformer le système *Madania*. Récemment, une convention entre le MALE et le MAS a également fait progresser le **mappage prévu entre l'IUC et l'IS** et des accords ont été conclus pour l'échange de données. Les projets de ces deux systèmes introduisent des progrès au niveau du respect de certaines normes internationales, telles que **l'engagement envers les standards ouverts et la neutralité technologique**. Et leurs architectures, en tant que **services et plateformes partagés**, peuvent être mises à profit par le gouvernement afin d'améliorer **la connexion entre les citoyens tunisiens et l'Etat**.

Au niveau des systèmes d'identification fonctionnels, le déploiement de l'IS et les améliorations qu'il connaît représentent une énorme **avancée de l'interopérabilité sectorielle et l'amélioration de l'identification des bénéficiaires des fonds sociaux**. Bien que le récent rapport d'audit a identifié certains problèmes persistants au niveau du système, le CRES a mis au point une stratégie pour en améliorer les performances. De plus, en enregistrant les bénéficiaires des programmes sociaux non contributifs (PNAFN et AMG1 / 2) et en les intégrant à l'IS, le MAS a fait les premiers pas vers la construction d'un registre social intégré qui pourrait servir de base à la protection sociale dans le pays.

³⁹ De cette manière, il pourrait fonctionner de la même manière qu'un système qui utilise la tokénisation pour limiter la propagation d'un identifiant unique, et stocke le mappage des tokens en identifiants dans un coffre-fort (comme par exemple, en Autriche) - voir la note de bas de page 50 pour plus d'explications.

En ce qui concerne l'assurance maladie, la carte basique à code-barres 2D qu'il est prévu de distribuer aux bénéficiaires de la CNAM **permettra l'authentification numérique et améliorera la sécurité et la facilité pour réaliser des transactions** à un coût inférieur aux solutions d'identification alternatives (par exemple, une carte à puce). Enfin, en choisissant d'étendre la carte CNAM aux détenteurs d'assurance maladie non contributifs (bénéficiaires du MAS), le GT pourra **éviter les coûts inutiles** associé au développement d'un système spécial d'identifiants pour ces programmes, et **assurer la protection de la vie privée des bénéficiaires du programme** en évitant de les distinguer par une carte différente. Si le pays choisissait de mettre en œuvre un programme de soins de santé universel, le système de cartes de la CNAM pourrait être adapté relativement facilement à cette fin.

Une demande certaine de services d'identification, d'authentification et de fiducie

Conformément aux priorités du PNS, la demande potentielle de services liés à l'identification et à l'authentification est forte - tant pour les agences publiques que pour les sociétés privées qui cherchent à digitaliser et à rationaliser leurs processus, à réduire la fraude et à permettre des services en ligne. Cela signifie que **les investissements dans l'IUC, les registres sectoriels et les services d'authentification numérique et de fiducie seront très appréciés, dans la mesure où ils répondent aux besoins de ces utilisateurs potentiels**. Il met également en évidence un certain nombre d'opportunités pour tester l'utilisation de l'IUC et des services d'authentification potentiels dans un avenir proche, y compris dans les secteurs suivants :

- **Les services administratifs en ligne (e-Government).** Une plate-forme d'authentification numérique est nécessaire pour permettre aux citoyens de se connecter en toute sécurité aux services d'administration en ligne pour un large éventail de secteurs, notamment la santé, l'éducation, la sécurité sociale et les filets de sécurité, la fiscalité et d'autres services administratifs.
- **La protection sociale.** Bien que l'IS assure actuellement l'interopérabilité et l'efficacité à l'intérieur du secteur de la protection sociale, la mise en correspondance de l'IS avec la base de données RIUC est essentielle pour faciliter la communication et l'échange de données avec d'autres secteurs et améliorer davantage les performances de ciblage en utilisant d'autres données administratives pour scruter le niveau de bien-être des ménages. En outre, certaines transactions du secteur social pourraient bénéficier d'une infrastructure d'authentification numérique offrant un niveau de garantie supérieur.
- **Éducation.** Comme indiqué ci-dessus, il existe actuellement un projet d'utilisation du RIUC pour l'inscription à l'école. Si ce système réussit, il sera étendu à toutes les écoles privées, ce qui pourrait faciliter la création d'un registre unique des élèves qui serait utile pour améliorer la gestion des écoles, y compris la détection des abandons scolaires, la gestion des programmes de bourses et la simplification des procédures pour les parents et les étudiants.
- **Réforme des subventions.** Le gouvernement envisage de concevoir un programme de transferts monétaires pour compenser les augmentations de prix dues à la suppression progressive des subventions aux produits alimentaires et énergétiques. Sur la base du plan actuel, les bénéficiaires de ce transfert monétaire devront être identifiés à minima par l'IS et une CIN (d'autres critères pourraient être utilisés comme par exemple la connexion au gaz pour la subvention énergétique ce qui impliquera un rapprochement / l'interopérabilité avec le SI de la STEG). En outre, un système d'authentification numérique sécurisée pourrait être utilisé pour aider à réduire les fraudes et les fuites lors de la distribution de paiements en espèces.
- **La santé.** Dans le cadre du projet en cours de modernisation des systèmes d'information hospitaliers, il a été décidé en 2019 lors d'un comité digital à la présidence du gouvernement que l'IS sera utilisé dans le secteur de la santé. D'autres possibilités de tirer parti du RIUC et / ou de l'authentification numérique pour la santé pourraient également être envisagées.

- **La réforme de la fonction publique.** L'IUC pourrait être mis en correspondance avec le système des ressources humaines et d'autres processus de back-end pour les fonctionnaires afin d'identifier de manière unique et précise chaque employé. Cela pourrait aider à garantir la déduplication et la suppression des postes « fantômes », ainsi qu'une identification cohérente lorsque les fonctionnaires se déplacent d'un département à l'autre.

En adoptant tout d'abord une vision multisectorielle, à moyen et à long terme de l'infrastructure d'identification et d'authentification numérique (voir ci-dessous), le GT sera davantage en mesure de contrôler de tels cas d'utilisation potentiels et de déterminer leur intérêt et leur faisabilité.

2. Principales faiblesses et risques

Incertitudes liées à la redevabilité du projet et à la gouvernance à long terme

Compte tenu du nombre de parties prenantes impliquées dans l'écosystème d'identité tunisien (voir Tableau 1 et Tableau 2), la gouvernance et la redevabilité des projets qui touchent à plusieurs secteurs sont parfois imprécises. Au-delà de la coordination des parties prenantes, **l'incertitude demeure quant à la gouvernance et à l'administration des projets spécifiques**. Pour l'IUC, par exemple, bien que la vision et les missions de l'OGI ont été délimités à la suite de plusieurs ateliers de travail entre différentes parties prenantes, ces dernières n'ont pas encore été formalisées par un décret d'application à cause du retard à promulguer la loi relative à la protection des données à caractère personnel (LPDP). Davantage **d'attention doit être en outre accordée au processus de gestion du changement entourant l'IUC et d'autres projets**, y compris les coûts d'adaptation pour diverses agences et les besoins en formation des fonctionnaires.

Enfin, le succès de la numérisation de l'identité, de l'authentification et de la prestation de services public en Tunisie **repose sur l'adoption de la LPDP et du code numérique**. En effet, si ces lois et leurs décrets d'application ne sont pas adoptés, les projets cités précédemment et de nombreux autres du PNS seront menacés.

Absence d'une vision holistique coordonnée de l'écosystème d'identité tunisien

Bien que le PNS offre une vue d'ensemble des divers projets et éléments nécessaires pour transformer la Tunisie en une société numérique, il n'existe **pas encore une vision claire partagée par toutes les parties prenantes de la façon dont tous les projets liés à l'identité - par exemple, l'IUC, l'IS, les solutions d'authentification numérique, TunXRoad, le portail unique des services etc. - fonctionneront ensemble et seront communément utilisés**. Bien que des projets tels que l'IUC soient régis par des comités multipartites, la collaboration interministérielle semble se faire projet par projet, avec une coordination intersectorielle réduite. En conséquence, la chronologie et la dépendance de certains projets a été difficile et a créé des inefficacités, et certaines décisions de conception sont en train d'être prises ad hoc plutôt qu'avec le grand dessein à l'esprit.

Bien que des progrès significatifs ont été accomplis dans la définition de la conception de l'IUC - par exemple, l'initialisation du registre et les récents protocoles d'entente signés respectivement entre le MALE et le MAS et le Ministère de l'éducation - il faut continuer l'implémentation des projets du SI IUC, la refonte de *Madania* et le cadre de l'interopérabilité nationale ainsi que les décrets d'application des lois LPDP et code du numérique pour entériner le rôle de l'OGI et de l'IUC dans l'écosystème national d'identification et authentification.

Des solutions d'authentification numérique limitées

Malgré l'élan enregistré pour le gouvernement numérique et les services électroniques, **la Tunisie manque actuellement de solutions ou de plateformes numériques déployées ou adoptées universellement et permettant une authentification sécurisée en ligne et en personne**. La CIN est le justificatif d'identité le plus utilisé par les adultes comme preuve d'identité. Toutefois, il s'agit généralement d'une simple inspection visuelle de la carte et de la photo de la personne. Dans sa forme actuelle, le système CIN n'offre pas l'infrastructure nationale ni les niveaux de garantie nécessaires à l'authentification numérique

en personne ou en ligne. En théorie, la carte à puce eCIN était censée combler cette lacune, mais le projet est au point mort et il est difficile de savoir si le ministère de l'Intérieur poursuivra cet effort et, le cas échéant, sous quelle forme.

En l'absence de l'eCIN, plusieurs **autres efforts et projets proposés impliquant l'Agence nationale de certification électronique (TUNTRUST)** ⁴⁰ **ont le potentiel d'améliorer l'infrastructure d'authentification du pays** et de répondre à la demande croissante de services électroniques :

- Les solutions la plus avancées sont développée par le MTCEN et TUNTRUST : un e-ID côté serveur appelé DigiGO sur format remote (Qualified Signature Creation Device) ⁴¹ et des certificats sous sur token cryptographique (Local Qualified Signature Creation Device). Le système DigiGO permettra aux utilisateurs de s'authentifier en fournissant un nom d'utilisateur et un mot de passe, ainsi qu'un mot de passe à usage unique envoyé à leur téléphone portable (SMS OTP). Également, TUNTRUST travaille actuellement avec le MALE pour mettre en place un système d'authentification au portail e-Service municipaux (en cours). Ces solutions peuvent faciliter l'authentification numérique et les signatures électroniques pour divers services des secteurs public et privé. Cependant, la couverture et l'utilisation de ces solutions sont faibles : 27 000 certificats issus sur token cryptographique.
- TUNTRUST travaille également sur une étude de faisabilité d'un « portefeuille citoyen » de documents primaires stockés (par exemple, permis de conduire, diplômes, bulletins de paie, etc.) pouvant être utilisés pour l'authentification via une application mobile.
- La CNI a également pris des initiatives pour collaborer avec les opérateurs de télécommunications afin d'identifier les citoyens via la technologie mobile.

Bien que ces services puissent potentiellement améliorer considérablement l'authentification numérique pour les services électroniques en ligne, ils ne résolvent pas (pour le moment) le problème de l'authentification sécurisée en personne, ce qui est nécessaire au moins à moyen terme, car la plupart des services publics tunisiens sont encore dispensés de manière directe et présente. Par exemple, la principale méthode actuelle d'authentification en personne consiste à examiner physiquement la carte CIN et à la comparer à la personne. Bien que la vérification du numéro CIN d'une personne (par exemple via le RIUC) puisse aider à établir l'exactitude des informations figurant sur la carte CIN, cela ne permet pas d'empêcher toute fraude d'identité et offre un niveau d'assurance inférieur à celui d'une solution utilisant la technologie numérique pour s'authentifier en sécurité.

En outre, il existe certaines limitations à l'adoption de solutions pour l'authentification en ligne en Tunisie. Par exemple, la quantité des services en lignes Egov est limitée, et il n'existe pas une obligation à l'utilisation de certificats électroniques ou de l'authentification forte pour d'autres transactions. Pour le développement d'un écosystème d'authentification numérique, les moyens d'inscription et de communications de l'ANCE restent limités (par exemple, communication, formation des agents terrains, etc.).⁴² En plus, il y a d'autres

40 TUNTRUST propose actuellement un certain nombre de services de certificats numériques et de signatures électroniques, notamment des certificats pour le système TUNEPS de passation des marchés publics, la déclaration électronique des taxes (système e-Jebaya), e-CNSS, CCPnet, les signatures électroniques pour les documents, etc. Ces services utilisent généralement des tokens (jetons) physiques, ce qui a limité leur utilisation ; Cependant, TUNTRUST étudie la possibilité que des utilisateurs d'entreprise stockent les certificats sur leurs propres serveurs ou les hébergent sur le serveur de TUNTRUST. Pour une liste de ces services, voir

<http://www.certification.tn/fr/nos-produits/id-trust-certificat-dauthentification-et-de-signature> et <http://www.certification.tn/fr/nos-produits/cachet-electronique-visible-tn-cev-2d-doc>.

41 Cet identifiant électronique est stocké sur le serveur de TUNTRUST et l'utilisateur peut accéder aux services à l'aide de l'ID de connexion, du mot de passe et du protocole OTP sur son téléphone. Dans le certificat il y a le CIN haché du porteur de certificat pour protection des données personnelles. Une copie de la carte CIN est fournie par le demandeur de certificat lors d'un entretien en face à face avec un agent de TUNTRUST pour s'assurer de l'identité du demandeur. <https://www.tuntrust.tn/fr/content/digigo>

42 Toutefois, une convention a été signée avec l'ANCE et une entreprise privée pour être une autorité d'enregistrement déléguée (<https://www.tuntrust.tn/fr/content/autorites-denregistrement-deleguees>) ce qui favorisera le déploiement de la solution DigiGO avec des F2F video en ligne. Cette solution sera opérationnelle après que la plateforme Manage PKI sera mise en œuvre (premier trimestre 2020).

limitations pour le déploiement d'une solution d'authentification qui utilise la technologie mobile. Bien que la couverture mobile en Tunisie soit élevée, elle n'en est pas encore à 100%. De nombreuses personnes partagent des téléphones mobiles et la vérification des identités des clients des opérateurs télécoms n'est pas assurée à 100% non plus, ce qui réduit le taux d'inclusion (et la sécurité) de l'utilisation des solutions d'identification mobile. Idéalement, les Tunisiens devraient disposer de plusieurs canaux d'authentification, fournisseurs et niveaux d'assurance parmi lesquels choisir afin de maximiser l'accessibilité et l'utilisation.

Problèmes connus liés à la qualité et à la précision des données

Un certain nombre de systèmes d'identification tunisiens doivent faire face à de **permanents défis de manque de qualité et d'exactitude de leurs données**, comme cela a été expliqué tout au long du présent rapport et résumé dans le Tableau 16.

Tableau 16 . Problèmes liés à la qualité et à la précision des données dans les systèmes clés

Système	Défis
Registre d'état civil (système Madania)	<ul style="list-style-type: none"> • Difficultés à séparer les chaînes de noms en arabe • Différences entre les noms arabes et latinisés • Erreurs de date de naissance • Plusieurs enregistrements du même acte civil (naissance, mariage et divorce) • Retards dans la mise à jour du système pour les naissances tardives et les événements d'état civil enregistrés à l'étranger • Erreurs de transcription du numéro de l'acte civil, ce qui n'inclut pas les sommes de contrôle • Les bases de données pour différents événements (naissances, mariages et décès) sont actuellement séparées, ce qui introduit davantage de possibilités d'erreurs et de doublons.
Carte d'identité nationale (CIN)	<ul style="list-style-type: none"> • Légalement, les citoyens sont tenus de mettre à jour leur CIN avec tout changement dans les informations. Cependant, comme la carte n'expire jamais, de nombreux citoyens ne doivent présenter une nouvelle demande que si leur carte est perdue. En conséquence, certains champs de données tels que l'adresse et la profession sont souvent obsolètes. • De plus, il est possible qu'une personne dispose de plusieurs cartes / numéros CIN ou que plusieurs personnes possèdent le même numéro CIN.
Identifiant unique de citoyen (IUC)	<ul style="list-style-type: none"> • Lors de l'initialisation du RIUC, les erreurs détectées entre <i>Madania</i> et la CIN ont été écartées et seront traitées à part (soit techniquement, soit via une campagne de fiabilisation des données par rapport aux données sur les registres de l'état civil qui nécessite un effort considérable avec l'aide de la Justice) • Il faut s'assurer que les SI clients (MAS et Ministère de l'éducation pour le moment) respectent le protocole établi pour ne pas permettre la création d'un identifiant fonctionnel sans passer par une vérification avec le RIUC et la création d'une correspondance entre les deux.
Identifiant social (IS)	<ul style="list-style-type: none"> • Les données de la CNRPS et de la CNSS, migrées vers la base de données CRES n'étaient pas toutes exactes. • Certains bénéficiaires ne peuvent pas se voir attribuer un IS car leurs enregistrements ne contiennent pas les huit critères utilisés pour la déduplication. • Le système d'information n'est pas directement lié à la base de données de <i>Madania</i> nécessaire pour garantir la mise à jour des informations sur les bénéficiaires (décès, départs à la retraite, etc.); Actuellement, les fonds valident les informations d'identité des nouveaux inscrits en utilisant <i>Madania</i>, mais ils ne reçoivent pas automatiquement les mises à jour lorsqu'un bénéficiaire est décédé. • Les conjoints mariés qui sont tous deux officiellement employés peuvent s'inscrire indépendamment dans les bases de données et ne peuvent pas être associés.

Des projets sont actuellement en cours pour améliorer la précision de la base de données de *Madania*, ainsi que des projets visant à accroître l'interopérabilité avec d'autres systèmes d'identification et à créer des grappes familiales, ainsi que la base de données IS. À court et à long terme, il sera essentiel de garantir la précision et la qualité des données stockées dans le système *Madania*, car le développement et l'intégrité des systèmes IUC et IS dépendront des données du registre d'état civil.

Faible interopérabilité et duplication continue de la collecte de données

Bien que la plupart des bases de données d'identité tunisiennes soient numériques, **le niveau d'intégration et d'interopérabilité est faible**. Même dans le secteur social - où l'IS facilite l'échange de données - les agences ou les programmes (CNSS, CNRPS, CNAM et MAS) collectent actuellement des informations pour leurs bénéficiaires séparément et créent des bases de données distinctes pour mettre en œuvre leurs programmes et services. En conséquence, il y a souvent un **chevauchement important des enregistrements d'identité, créant des redondances et des erreurs potentielles, ainsi que des inefficacités administratives lors de la transition d'un programme à un autre**. La mise en œuvre de l'IS a permis de réduire bon nombre de ces problèmes, en rationalisant la vérification des identités entre les systèmes. Cependant, cela n'a pas réduit les redondances dans les activités de collecte de données, en particulier pour les données économiques et sociales qui vont au-delà de l'identité de base d'une personne. La collecte de données en double nécessite non seulement des ressources en double, mais peut également créer des erreurs et des divergences entre les systèmes. Elle peut également constituer un risque pour la protection des données et la vie privée en traitant inutilement les données à caractère personnel.

La mise en œuvre du projets et les retards législatifs pourraient créer de nouveaux problèmes

La plupart des projets en cours concernant l'identité et des éléments plus larges de la stratégie de transformation numérique définie dans le PNS sont **interdépendants et nécessitent l'adoption du LPDP et du code numérique**. Des retards dans le déploiement de projets de base ou dans l'adoption de lois essentielles et dans la mise en œuvre de décrets pourraient limiter le succès du projet. Par exemple, la plate-forme TunXRoad proposée est une colonne vertébrale essentielle de l'échange de données entre les agences gouvernementales, et elle est nécessaire pour que l'IUC atteigne son potentiel, de même que des améliorations du système *Madania*. En outre, des solutions d'authentification numérique avec différents niveaux de garantie sont nécessaires pour déployer des services électroniques, gérer le contrôle d'accès pour des systèmes tels que IUC, IS et *Madania*, permettre aux utilisateurs de se connecter au portail citoyen de l'IUC et renforcer la sécurité pour des utilisateurs des services personnalisés, comme l'ouverture d'un compte bancaire ou de téléphone portable. Des retards dans la mise en œuvre des solutions d'authentification numérique de base pourraient donc bloquer ces services, ou conduire à une prolifération de systèmes d'identification numérique cloisonnés, spécifiques à chaque secteur et non interopérables.

3. Recommandations

Mettre en place un comité multipartite pour synchroniser les projets et fournir une vision globale de l'avenir de l'identification en Tunisie

Afin d'améliorer la coordination et d'obtenir les recommandations supplémentaires ci-dessous, **le GT devrait convoquer un large groupe de parties prenantes pour les projets d'identification et d'authentification en cours.** Cela pourrait être fait sous la direction du MTCEN et du MALE et inclure au minimum toutes les autres parties prenantes détaillés dans les tableaux 1 et 2 (CNI, ANCE, INPDP, police technique, ministère de l'Intérieur, MAS, CRES, CNRPS, CNSS, CNAM, Ministère des finances, ISIE, l'UAE, etc.), les organismes publics potentiellement utilisateurs de systèmes d'identité (ministères de la santé, de l'éducation, de l'enseignement supérieur, etc.), administrations locales, secteur privé (banques et opérateurs mobiles) et des représentants de la société civile. Les objectifs initiaux de cet exercice seraient les suivants :

- S'assurer que tous les participants connaissent le statut et les plans de toutes les initiatives en cours et peuvent les associer à d'autres projets en cours (par exemple, services en ligne, réformes administratives, Maison de service, etc.).
- Trouver des opportunités de collaboration, favoriser les contributions concernant ces projets sous différents angles et envisager d'autres domaines de coopération.
- Trouver de nouveaux mécanismes pour assurer la saisie et l'optimisation continues des projets d'identification afin qu'ils répondent aux besoins des différents secteurs et des citoyens.
- Déterminer clairement les responsabilités pour chaque projet tout en maintenant ces projets coopératifs et multisectoriels.
- Veiller à ce que les ressources engagées soient allouées à la formation et au soutien des responsables et divers autres utilisateurs lors de la mise en œuvre de nouveaux systèmes afin de garantir un processus de gestion du changement sans heurts.

En outre - et en complément de cette vision large de la Tunisie numérique proposée par le PNS - ce groupe de parties prenantes devrait **travailler à définir une vision plus spécifique à moyen et à long terme relative à l'infrastructure d'identification et d'authentification.** Par exemple :

- À quoi devrait ressembler l'identité numérique dans 5 ou 10 ans du point de vue (1) des fournisseurs d'identité (par exemple, le MALE, l'OGI, l'ANCE, la police technique, etc.), (2) des différents organismes gouvernementaux (par exemple, les secteurs sociaux, sanitaires, l'éducation, la fiscalité, l'administration électorale, etc.), (3) des citoyens et (4) du secteur privé ?
- Comment une identification, une interopérabilité et une authentification uniques améliorées peuvent-elles répondre à des objectifs plus larges, tels que l'instauration d'un climat de confiance, la capacité et l'innovation des fournisseurs de services et l'amélioration du développement inclusif ?
- Quelles seront idéalement les interactions d'une personne avec les systèmes d'identification tout au long de son parcours, de la naissance au décès ?
- Comment la Tunisie veillera-t-elle à ce que les citoyens aient le choix, le contrôle et la supervision de leurs données d'identité, conformément aux normes internationales ?
- Comment chacun des projets existants répondra-t-il à la vision exprimée ci-dessus ? Quelles lacunes ou préoccupations doivent encore être abordées ? Cela nécessite-il de nouveaux projets ou d'une révision des systèmes actuels ? Peut-on mieux harmoniser les projets et les choix technologiques pour améliorer l'efficacité et la durabilité ?

- Au-delà de ces grandes questions, un groupe multipartite devrait être consulté sur la suite donnée aux recommandations ultérieures. En outre, les indicateurs de redevabilité concernant la mise en œuvre de cette vision, ainsi que les composants individuels du produit doivent être clairement définis et compris par toutes les parties.

Veiller à ce que la conception de l'IUC se traduise par un système fiable, inclusif et utile

Lorsqu'il est exploité par différents secteurs, un registre d'identifiants unique comme le RIUC peut aider les fournisseurs de services à améliorer les processus back-end qu'ils utilisent pour identifier les citoyens, les bénéficiaires et les clients, en réduisant les fraudes et en augmentant l'efficacité. En outre, cela peut également aider à faciliter de nouveaux modes de prestation de services et à simplifier les procédures administratives front-end des particuliers.

Cependant, pour jouer ce rôle, l'IUC doit être **inclusif** (c'est-à-dire couvrir toute la population), **objet de confiance** (c.-à-d. être fiable, sécurisé et responsable), et **conçu pour apporter une valeur ajoutée aux personnes et aux institutions**.

Comme décrit dans la partie 2, Tableau 13, le système IUC prévoit déjà de déployer un certain nombre de services sur une base pilote. Nous recommandons que le GT s'appuie sur ce cadre en **identifiant à la fois une vision à long terme et des plans sectoriels sur la manière dont l'IUC peut être exploité et intégré dans différents systèmes et processus sectoriels**.

Tableau 17 . Avantages potentiels d'un registre d'identités unique pour la prestation de services

Catégorie	Les avantages
Efficacité administrative	<p>Une fois mappés sur les identifiants sectoriels — ex, pour la protection sociale, les taxes, etc. - des identifiants uniques peuvent automatiser les requêtes d'identité, réduisant ainsi le temps, la main-d'œuvre et le potentiel d'erreur humaine. Cela comprend l'automatisation :</p> <ul style="list-style-type: none"> • de la vérification des données d'identité de base par rapport à la base de données d'identité unique (p. Ex. Confirmation de la date de naissance d'un nouveau bénéficiaire) • de l'échange de données et requêtes entre des bases de données fonctionnelles (par exemple, vérification des enregistrements du registre de propriété pour un contribuable)
Réduction de la fraude et amélioration du ciblage	<p>En établissant l'unicité et facilitant l'interopérabilité, l'identité unique peut être exploitée par plusieurs secteurs pour réduire les erreurs d'inclusion et d'exclusion en fournissant :</p> <ul style="list-style-type: none"> • une identité unique vérifiée pour les nouveaux inscrits peut éliminer les doublons • des informations actualisées sur les décès, fournies par des liens vers l'état civil peuvent aider à éliminer les fantômes • et en permettant l'échange de données entre différentes bases de données sectorielles (par exemple, l'administration fiscale et la sécurité sociale) peut augmenter l'information disponible pour prendre des décisions en matière d'éligibilité concernant une personne.
Services plus faciles d'utilisation	<p>Si l'utilisation finale de l'identité unique sert à simplifier les processus front-end, cela peut améliorer le confort de l'utilisateur en :</p> <ul style="list-style-type: none"> • Réduisant le nombre de documents nécessaires pour vous inscrire à un programme ou vérifier votre identité (par exemple, pour le CIN, une personne doit présenter un acte de naissance, un certificat de nationalité, un certificat de travail, etc.).

Pour chaque secteur et chaque cas d'utilisation prioritaire potentiel tel que la **gouvernance électronique, la protection sociale, la réforme des subventions, la santé et l'éducation, la fonction publique**, les parties prenantes pourraient **évaluer les avantages potentiels dans trois catégories montrées dans le Tableau 17**, en considérant ce qui suit :

- Comment le RIUC pourrait-il être utilisé pour (a) améliorer l'efficacité administrative, (b) réduire la fraude et améliorer le ciblage ?
- Comment les améliorations back-end utilisant le RIUC peuvent-elles également se traduire par des services plus pratiques à utiliser pour les citoyens ? (par exemple, en éliminant la nécessité pour eux d'apporter des copies physiques de documents tels que les certificats de naissance lors de l'inscription à un programme)
- Quelles lois et / ou quels décrets gouvernementaux doivent être modifiés ou mis à jour pour faciliter ces nouveaux modes de prestation de services ?
- Quelles ressources faut-il engager pour que différents secteurs utilisent le RIUC (par exemple, mises à jour nécessaires du système, intégration, formation, réingénierie des processus métier, etc.) ?
- Plus généralement, les parties prenantes devraient également définir des options pour savoir :
- Si les services en ligne seront disponibles via un portail gouvernemental unique et/ou si chaque ministère exploitera son propre portail.
- Si une plate-forme de services électroniques formera un portail unique avec celui par lequel les citoyens accéderont aux données des personnes qui ont utilisé leurs informations d'identité (comme requis par le cadre juridique de l'IUC)
- Si les services de vérification du RIUC seront éventuellement disponibles pour le secteur privé (par exemple, pour répondre aux exigences de type KYC (connaissez votre client) des banques)

Gardant à l'esprit cette vision et ces cas d'utilisation, le gouvernement tunisien devrait continuer l'édification de **l'IUC de manière à répondre aux besoins des utilisateurs sectoriels et du peuple tunisien, en incluant toute la population et en faisant en sorte de créer un système dans lequel les individus et les institutions ont confiance**. Les principales questions à prendre en compte sont notamment :

- Comment inclure le faible pourcentage de citoyens qui n'ont jamais été enregistrés à la naissance (probablement ceux des zones rurales) ?
- Comment inclure éventuellement des non-citoyens ?
- La structure de gouvernance de l'OGI : À qui répondra-t-il ? Comment sera-t-il administré ? Comment sera-t-il financé ?
- Quel rôle jouera l'IUC dans TunXRoad ? Le RIUC facilitera-t-il les requêtes entre différentes bases de données (par exemple, si l'administration fiscale a besoin de demander des informations à la MAS) ?
- Comment l'IUC sera-t-il mappé avec d'autres identifiants existants (par exemple, pour l'administration fiscale) ?
- Comment l'IUC sera-t-il mappé avec des bases de données qui n'ont pas encore d'identifiant (par exemple, les hôpitaux, les écoles) ?
- Qui fournira les ressources aux utilisateurs du système - le MAS, le ministère de la Santé, de l'Éducation, des Finances, etc. - pour qu'ils puissent adapter et / ou numériser leurs bases de données afin d'utiliser le cadre d'interopérabilité ?
- Quels processus de gestion du changement seront adoptés pour faire en sorte que les fonctionnaires et les citoyens prennent conscience du nouveau système et soient incités à s'y conformer ?

- Quels mécanismes de règlement des réclamations seront adoptés pour garantir que tous les citoyens - y compris ceux qui ont peu de chances d'accéder à un portail en ligne - soient en mesure d'enregistrer des réclamations et de corriger facilement les erreurs concernant leurs données ou leur utilisation ?

Donner la priorité aux réformes du registre d'état civil et du cadre d'interopérabilité national

Les améliorations apportées au registre d'état civil et la mise en place d'un cadre national d'interopérabilité sont des catalyseurs essentiels du RIUC et d'autres projets et services liés à l'identité. Renforcer la qualité et l'utilité du registre d'état civil est un élément fondamental pour assurer un écosystème d'identité inclusif et fiable. En outre, le projet d'interopérabilité national - appelé TunXRoad et promu par le MTCEN - constitue l'un des objectifs centraux du PNS et il est essentiel pour garantir que l'IUC puisse être largement utilisé dans le secteur public.⁴³

Comme indiqué dans la partie 2, le MALE a déjà élaboré une stratégie visant à améliorer la qualité et la précision des données dans le système *Madania*, en appui au RIUC, ainsi que le développement de clusters familiaux. Cette stratégie comprend également une mise à niveau de la conception du système afin de le rendre plus fiable, sécurisé, interopérable et utile pour différentes agences, notamment le ministère de la Santé, le ministère des Affaires étrangères, le ministère de la Justice et l'INS. La poursuite des progrès et l'engagement dans ces efforts sont essentiels pour assurer la qualité et l'intégrité des systèmes d'identification tunisiens.

Accélérer le développement de solutions d'authentification numérique

Comme décrit ci-dessus, un certain nombre de projets liés à l'authentification sont actuellement en cours, à différents stades de développement. **Cependant, une réflexion plus holistique est nécessaire afin de garantir que les systèmes d'authentification planifiés (a) répondent aux besoins des différents utilisateurs et des types de transaction futurs, notamment en fournissant les niveaux de garantie appropriés, (b) soient économiques et interopérables, et (c) soient accessibles à l'ensemble de la population. Un groupe multipartite (comme décrit ci-dessus) devrait réfléchir :**

- A la manière d'améliorer les processus actuels d'authentification des citoyens pour les transactions présentielle en termes d'efficacité, de sécurité et de commodité.
- aux besoins immédiats et futurs d'authentification en ligne (par exemple, pour les services électroniques) de différents segments de la population.
- Aux niveaux de garantie nécessaires pour différents types de transactions, conformément aux meilleures pratiques internationales.
- Aux avantages et inconvénients de différents types de facteurs et de mécanismes d'authentification (cartes, cloud, mobile, jetons, etc.) en ce qui concerne (1) l'accessibilité pour la majorité de la population, (2) la sécurité et les niveaux de garantie, et (3) le coût.

⁴³ À notre connaissance, cette couche d'interopérabilité sera calquée sur le système estonien X-Road <https://e-estonia.com/solutions/interoperability-services/x-road>, mais on ignore dans quelle mesure il suivra sa conception. Le système X-Road est placé à la base des services d'identité électronique et d'administration en ligne de l'Estonie pour faciliter les requêtes et le transfert de données entre bases de données. En utilisant un identifiant unique (le PIC ou code d'identification personnel) attribué à chaque résident en tant que clé, le système X-Road relie des centaines de systèmes publics et privés qui conservent chacun leur souveraineté, et échangent des données et des requêtes sur la base d'accords. Une caractéristique notable du système est qu'en droit estonien, aucune base de données connectée à X-Road n'est autorisée à collecter des informations d'identité déjà contenues dans l'une des bases de données connectées, ces informations étant disponibles via la couche d'interopérabilité, ce qui élimine une collecte double des données.

- A la manière avec laquelle les différentes solutions d'authentification numérique (p. Ex. DigiGO, une carte d'identité électronique potentielle, des solutions du secteur privé, etc.) interagiront et / ou établiront un groupe de fournisseurs d'identité numérique ?
- Comment construire des systèmes d'authentification avec des mesures appropriées de « respect de la vie privée dès la conception » pour assurer le contrôle de l'utilisateur et la protection des données (voir recommandation ultérieure)
- Comment l'authentification numérique peut-elle être exploitée pour les paiements électroniques potentiels pour divers transferts monétaires du gouvernement aux particuliers
- Si les solutions d'identification numérique fournies par le gouvernement peuvent être utilisées par le secteur privé (par exemple, pour les exigences KYC), secteur qui sera le principal utilisateur de l'authentification numérique et encouragera son adoption.
- Comment élargir l'écosystème de fournisseurs potentiels d'identification et d'authentification numérique, y compris au secteur privé

Contrairement aux systèmes d'identification uniques comme *Aadhaar* en Inde, l'**IUC tel qu'il est actuellement conçu, ne peut pas être utilisé comme identifiant pour l'authentification en ligne, sans carte**. La LPD, en effet, interdit que le numéro IUC soit rendu public ou imprimé sur des identifiants (ce qui est permis pour les numéros de CIN). Cela signifie que les citoyens ne connaîtront ni ne verront jamais leur numéro. Cependant, en théorie, un fournisseur d'identité (par exemple, le MALE, l'OGI ou l'ANCE) pourrait tokéniser l'IUC (bâtir dessus un système de jetons) ce qui permettrait de remplacer l'IUC par un numéro généré de manière aléatoire, sans lien avec l'IUC - et fournir ces jetons aux citoyens sans compromettre le secret de l'IUC.⁴⁴ Afin de tirer parti de ce numéro IUC avec jetons comme identifiant pour l'authentification, les personnes doivent toujours s'enregistrer pour recevoir le numéro et recevoir des mécanismes et facteurs d'authentification (cartes, mots de passe, codes confidentiels, données biométriques, etc.) pour prouver leur identité en ligne.

Renforcer les systèmes d'information et les registres sectoriels lors de la planification de l'intégration aux systèmes nationaux

Afin de tirer parti de l'IUC, de l'authentification numérique et de TunXRoad, les programmes et services existants devront **développer des systèmes back-end numérisés et interopérables**.

Dans certains cas, tel que celui de la santé où les registres centralisés des utilisateurs (patients) n'existent pas encore, des investissements importants sont nécessaires pour développer des systèmes d'information et d'autres infrastructures nécessaires pour se connecter aux plateformes nationales et créer des services électroniques qui peuvent utiliser les services d'authentification numérique et de confiance. Dans d'autres cas, tels que les programmes de protection sociale, il existe déjà un système bien développé avec une interopérabilité sectorielle facilitée par l'IS (voir Encadré 4 pour plus de détails sur les recommandations pour le secteur de la protection sociale). Même dans ce dernier cas, cependant, la planification et l'investissement sont nécessaires pour intégrer les systèmes existants avec l'IUC et TunXRoad à l'avenir. Dans certains cas - par exemple, l'IS -, les agences ont jugé nécessaire de développer des systèmes parallèles pour répondre aux besoins immédiats avant que les plateformes nationales se soient développées. Dans la mesure du possible, toutefois, toutes les solutions à court terme doivent être conçues dans une optique à long terme afin de garantir l'interopérabilité future et d'éviter le doublement des investissements.

44 La *tokénisation* est un processus de « pseudonymisation » qui implique de prendre un identifiant sensible (par exemple, un identifiant unique ou un numéro de carte de crédit) et d'appliquer un algorithme pour le mapper sur un nouvel identifiant non sensible (appelé « jeton »). Si le jeton est compromis (par exemple, si l'identité est volée), le voleur aurait la possibilité de procéder à une ingénierie inverse du vrai numéro d'identification et le fournisseur d'identité pourrait simplement délivrer un nouveau jeton.

Encadré 4 . Renforcement des systèmes de protection sociale - vers un registre social intégré

Pour renforcer les systèmes de protection sociale, les principales étapes recommandées sont résumées ci-dessous.

Améliorer la qualité des données (identifiant social). Alors que l'identifiant social (IS) est attribué à 10 millions d'enregistrements, il reste encore des problèmes de qualité des données à traiter en termes d'unicité d'identités et de cohérence des informations dans différentes bases de données. Une évaluation récente a identifié un certain nombre de plans d'action^a qui soulignent l'importance des arrangements institutionnels et d'une coordination plus étroite et d'un effort concerté de toutes les parties prenantes.

Élargir la couverture du registre. Actuellement, le registre des bénéficiaires du MAS comprend 20% de la population (environ 600 000 ménages). Au-delà des bénéficiaires actuels des principaux programmes de protection sociale, il est recommandé d'étendre la couverture à d'autres programmes et à un plus grand nombre de bénéficiaires potentiels, en vue de la mise en place d'un registre social intégré (voir ci-dessous).

Mettre en place une nouvelle approche de ciblage. S'appuyant sur la nouvelle loi sur la protection sociale qui stipule l'utilisation de scores et de critères objectifs pour évaluer les bénéficiaires potentiels - le gouvernement doit approuver officiellement la nouvelle approche de ciblage pour rendre son action plus opérationnelle au niveau de la sélection et de l'évaluation des bénéficiaires de programmes de protection sociale. Parallèlement, d'autres systèmes de traitement et d'information doivent être mis en place pour faciliter le suivi des bénéficiaires, le paiement, les réponses aux réclamations, etc.

Une plus grande interopérabilité et intégration au-delà des secteurs, en liaison avec la plateforme nationale. Le ciblage (identification initiale et réévaluation) s'améliorera avec le temps, car davantage de données administratives seront liées et mises à la disposition du MAS afin de vérifier le statut socioéconomique des personnes. En règle générale, ces données administratives clés comprennent le registre d'état civil, les impôts, les terres, les biens et la sécurité sociale. Pour réaliser l'interopérabilité et l'intégration, en particulier avec le niveau national (c'est-à-dire en utilisant l'IS et l'IUC), les protocoles doivent être définis et convenus avec toutes les parties concernées et être conformes au cadre juridique actuel et futur.

Mettre en place une authentification améliorée grâce à une nouvelle carte à code à barres. Le MAS / la CNAM a commencé à distribuer de nouvelles cartes de santé / protection sociale (cartes CNAM) aux bénéficiaires du programme d'assurance maladie ordinaire (contributif) et des bénéficiaires du programme pour personnes souffrant d'une carence sanitaire (bénéficiaires d'un programme d'aide sociale non contributif). Son entrée en usage étant toujours en attente, le processus opérationnel doit être mis en place progressivement. De plus, ce cas d'utilisation sectorielle doit être étroitement coordonné avec les mécanismes nationaux d'authentification en cours de discussion.

Un **Registre Social Intégré (RSI)** est un système qui fournit une source commune d'informations sur les bénéficiaires existants et potentiels de multiples programmes et / ou services. À l'aide de paramètres propres à chaque programme d'assistance sociale ou autre, les administrateurs peuvent simplement interroger l'ISR pour obtenir des données sur les personnes, correspondant à leurs critères d'éligibilité spécifiques. En d'autres termes, différents programmes et services n'ont pas besoin de collecter eux-mêmes de nouvelles données pour sélectionner leurs bénéficiaires. Cela peut améliorer l'efficacité, générer des économies financières et réduire le fardeau imposé aux individus en éliminant les efforts redondants, coûteux et fastidieux de collecte, de vérification et de gestion des données. Combinés à une plateforme d'interopérabilité permettant l'échange de données et l'interrogation avec d'autres secteurs (fiscalité, sécurité sociale, foncier et immobilier, registres, etc.), les gains d'efficacité peuvent être encore plus importants.

a. Talys Consulting and CRES. "CRES - Feuille de route des projet." (presentation).

Protéger les données et la confidentialité dès / et par le biais de la conception

Comme indiqué ci-dessus, l'architecture globale du système IUC inclut déjà certaines conceptions protégeant la confidentialité (par exemple, limitant la distribution de l'IUC et du portail d'accès utilisateur), de même que certaines des mises à niveau planifiées du système *Madania* (par exemple, cryptage et contrôles de sécurité améliorés). En outre, la nouvelle loi sur la protection des données (LPDP) définit des paramètres essentiels de l'IUC et de son utilisation, ainsi que des réglementations plus larges sur le traitement des données à caractère personnel par d'autres acteurs des secteurs public et privé.

Le respect de ces règles sera essentiel pour assurer le succès non seulement de l'IUC, mais également de la collecte, du stockage, de l'utilisation et de l'échange de données inhérentes à d'autres projets, notamment les solutions IS, TunXRoad et celles d'authentification numérique. Cela nécessite non seulement une surveillance continue de l'INPDP, mais également un engagement plus large avec différents acteurs gouvernementaux, du secteur privé et de la société civile afin de s'assurer que ces réglementations soient pleinement comprises et appliquées.

En outre, et conformément à la loi, le gouvernement devrait également **travailler à la mise en place de contrôles opérationnels et techniques supplémentaires afin de garantir que les données et la confidentialité soient protégées par défaut** dans tout système qui traite des données personnelles, telles que l'IUC, *Madania*, la CIN, les registres sectoriels tels que le système d'information, les solutions d'authentification telles que DigiGO et la carte de la CNAM, etc. Parmi ces mesures on peut citer notamment les stratégies et les solutions présentées dans le Tableau 18 .⁴⁵ En outre, il est recommandé que le GT mène **des évaluations supplémentaires d'impact sur la vie privée et des exercices de modélisation des menaces** afin d'évaluer l'impact et les risques des systèmes actuels et futurs sur la sécurité des données des personnes.

Tableau 18 . Exemples de technologies et de contrôles opérationnels renforçant la confidentialité

La stratégie		Exemple de solutions (non exhaustif)
Orienté données	Minimiser la collecte et le traitement des données personnelles pour limiter l'impact du système sur la vie privée	<ul style="list-style-type: none"> Collecte et partage de données minimales Anonymisation et utilisation de pseudonymes lors du traitement de données
	Masquer les données personnelles et leurs interrelations en vue de rendre impossible la liaison et l'observabilité, en minimisant les abus potentiels	<ul style="list-style-type: none"> Crypter les données stockées ou en transit Cryptage de bout en bout Gestion et anonymisation des clés Anonymisation et utilisation de pseudonymes ou de token (jetons) pour le traitement de données Approche de type "Zéro sémantique" : numéros d'identification générés aléatoirement (non séquentiels ou significatifs) Pièces d'identité basées sur les attributs (ABCs)
	Séparer , compartimenter ou distribuer le traitement des données personnelles chaque fois que possible pour atteindre le but recherché et éviter la possibilité de faire des profils complets d'individus	<ul style="list-style-type: none"> Tokénisation ou pseudonymisation par secteur Séparation logique et physique des données (par exemple, biographique ou biométrique) Vérification fédérée ou décentralisée

45 Voir aussi Banque mondiale. 2018 « Protection de la vie privée dès la conception : pratiques en vigueur en Estonie, en Inde et en Autriche ». Washington, DC: Banque mondiale. <http://documents.worldbank.org/curated/en/546691543847931842/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria>.

	La stratégie	Exemple de solutions (non exhaustif)
	Agréger les données personnelles au niveau le plus élevé possible lors du traitement afin de limiter la quantité de données personnelles restantes.	<ul style="list-style-type: none"> Anonymiser les données en utilisant « l'anonymat k », la confidentialité différentielle et d'autres techniques (par exemple, agréger des données au fil du temps, réduire la granularité des données de localisation, etc.)
Orienté processus	Inform er les individus chaque fois que leurs données sont traitées, dans quel but elles le sont et par quels moyens	<ul style="list-style-type: none"> Notifications de transaction Notifications de violation de données
	Donner aux individus des outils pour contrôler le traitement de leurs données, mettre en œuvre les droits de protection des données et améliorer la qualité et la précision des données	<ul style="list-style-type: none"> Services d'identité centrés sur l'utilisateur Informations d'identification basées sur les attributs
	Appliquer une politique de confidentialité et de protection des données conforme aux exigences légales	<ul style="list-style-type: none"> Contrôle d'accès basé sur les rôles avec authentification à deux facteurs Accès à distance Mesures physiques et cyber sécurité
	Démontrer un respect sans faille de la politique de confidentialité et des exigences légales applicables	<ul style="list-style-type: none"> Journaux inviolables Audits

Source : Tableau adapté du Guide du praticien ID4D (www.id4d.worldbank.org/guide). Cadre original adapté de <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> pour s'adapter au contexte du système d'identification.

Remarque : ce tableau est censé illustrer les technologies de contrôle opérationnels les plus courants, mais il n'est pas exhaustif.

id4d.worldbank.org

