Public Disclosure Authorized
Public Disclosure Authorized
Public Disclosure Authorized
Public Disclosure Authorized

ID4D
Diagnostic of ID Systems in Tunisia

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP

© 2019 International Bank for Reconstruction and Development/The World Bank
1818 H Street, NW, Washington, D.C., 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Some Rights Reserved

This work is a product of the staff of The World Bank with external contributions. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of The World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Nothing herein shall constitute or be considered to be a limitation upon or waiver of the privileges and immunities of The World Bank, or of any participating organization to which such privileges and immunities may apply, all of which are specifically reserved.

Rights and Permission

This work is available under the Creative Commons Attribution 3.0 IGO license (CC BY 3.0 IGO) http://creativecommons.org/licenses/by/3.0/igo. Under the Creative Commons Attribution license, you are free to copy, distribute, transmit, and adapt this work, including for commercial purposes, under the following conditions:

Attribution—Please cite the work as follows: World Bank. 2020. *Identification for Development (ID4D): Diagnostic of ID Systems in Tunisia,* Washington, DC: World Bank License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

Translations—If you create a translation of this work, please add the following disclaimer along with the attribution*: This translation was not created by The World Bank and should not be considered an official World Bank translation. The World Bank shall not be liable for any content or error in this translation.*

Adaptations—If you create an adaptation of this work, please add the following disclaimer along with the attribution: *This is an adaptation of an original work by The World Bank. Views and opinions expressed in the adaptation are the sole responsibility of the author or authors of the adaptation and are not endorsed by The World Bank.*

Third Party Content—The World Bank does not necessarily own each component of the content contained within the work. The World Bank therefore does not warrant that the use of any third-party-owned individual component or part contained in the work will not infringe on the rights of those third parties. The risk of claims resulting from such infringement rests solely with you. If you wish to reuse a component of the work, it is your responsibility to determine whether permission is needed for that reuse and to obtain permission from the copyright owner. Examples of components can include, but are not limited to, tables, figures, or images.

All queries on rights and licenses should be addressed to World Bank Publications, The World Bank, 1818 H Street, NW, Washington, DC, 20433; USA; email: pubrights@worldbank.org.

Cover photo credits: (Top circle) Tom Perry / World Bank, (Center and bottom circles) Arne Hoel / World Bank.

Contents

Tables

Figures

About ID4D

The World Bank Group's Identification for Development (ID4D) Initiative uses global knowledge and expertise across sectors to help countries realize the transformational potential of digital identification systems to achieve the Sustainable Development Goals. It operates across the World Bank Group with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and legal, among others.

The mission of ID4D is to enable all people to access services and exercise their rights by increasing the number of people who have an official form of identification. ID4D makes this happen through its three pillars of work: thought leadership and analytics to generate evidence and fill knowledge gaps; global platforms and convening to amplify good practices, collaborate, and raise awareness; and country and regional action to provide financial and technical assistance for the implementation of robust, inclusive, and responsible digital identification systems that are integrated with civil registration.

The work of ID4D is made possible with support from the World Bank Group, Bill & Melinda Gates Foundation, the UK Government, the French Government, the Australian Government and the Omidyar Network.

To find out more about ID4D, visit id4d.worldbank.org. To participate in the conversation on social media, use the hashtag #ID4D.

Acknowledgments

This report was prepared by Julia Clark, Aziz Ben Ghachem, and Yuko Okamura on behalf of the World Banks' Identification for Development (ID4D) initiative, and benefited greatly from feedback and inputs by Simon O'Meally, Axel Rifon Pérez, Carlo Rossotto, Mahdi Barouni, Julian Najles, and David Satola.

The report would not have been possible without the contributions of many members of the Tunisian government who generously provided their expertise and time to facilitate this mission. This includes members of the Ministry of Communications Technologies and Digital Economy (MTCEN), the Ministry of Local Affairs and the Environment (MALE), the Ministry of Social Affairs (MAS), the National Pension and Social Insurance Fund (CNRPS), the National Social Security Fund (CNSS), the National Health Insurance Fund (CNAM), the Center for Research and Social Studies (CRES), the National Informatics Center (CNI), the national digital certificate agency (TUNTRUST), the President's Office, the Ministry of Health, and the Ministry of Education, and the National Authority for the Protection of Personal Data (INPDP). In addition, the Ministry of Development Investment and International Cooperation (MDICI) was instrumental in helping to facilitate this mission and the completion of the report.

Abbreviations

API	application program interface
CIN	*Carte d'identité nationale* [national ID card]
CNAM	*Caisse nationale d'assurance maladie* [National Health Insurance Fund]
CNI	*Centre national de l'informatique* [National Informatics Center]
CNRPS	*Caisse nationale de retraite et de prévoyance sociale* [National Pension and Social Insurance Fund]
CNSS	*Caisse nationale de sécurité sociale* [National Social Security Fund]
CNTE	*Centre National des Technologies de L'Education* [National Center of Education Technologies]
CR	civil registry
CRES	*Centre des recherches et des études sociales* [Center for Research and Social Studies]
(e)KYC	(electronic) Know Your Customer
GDPR	General Data Protection Regulation
GoT	Government of Tunisia
INPDP	*Instance nationale de protection des données personnelles* [National Authority for the Protection of Personal Data]
INS	*L'Institut National de la Statistique* [National Institute of Statistics]
ISIE	*Instance supérieure indépendante pour les élections* [High Independent Authority for Elections]
IS	*Identifiant social* [social identifier]
IUC	*Identifiant unique citoyen* [unique citizen identifier]
LPDP	*Loi relative à la protection des données personnelles* [law on the protection of personal data]
MALE	*Ministère des affaires locales et de l'environnement* [Ministry of Local Affairs and the Environment]
MAS	*Ministère des affaires sociales* [Ministry of Social Affairs]
MOH	Ministry of Health
MOI	Ministry of Interior
MTCEN	*Ministère des technologies de la communication et de l'économie numérique* [Ministry of Communications Technologies and Digital Economy]

NID	national ID
OGI	*Organe de Gestion de l'IUC* [IUC Management Body]
OTP	one-time password
PG	*Présidence du gouvernement* [President's Office]
PKI	public key infrastructure
PNAFN	*Le Programme National d'Aide aux Familles Nécessiteuses* [National Assistance Program for Families in Need]
PNS	*Plan national stratégique* [national strategic plan]
RIUC	*Registre de l'Identifiant Unique du Citoyen* [Unique Citizen Identifier Registry]
TUNTRUST	*Agence nationale de certification electronique* [National Agency for Electronic Certification or ANCE]
UAE	*Unité de l'administration électronique* [Electronic Administration Unit]
UIN	unique identity number

Executive Summary

Introduction

This report presents the current state of identification (ID) systems in Tunisia and their use across sectors. Based on an initial study completed in 2018 by the World Bank's Identification for Development (ID4D) Initiative, it provides a summary of the strengths and weakness of the country's primary ID systems and recommended next steps for developing an inclusive and trusted identity ecosystem that will improve governance and facilitate access to basic rights and services.

Identification in Tunisia: Assets and Gaps

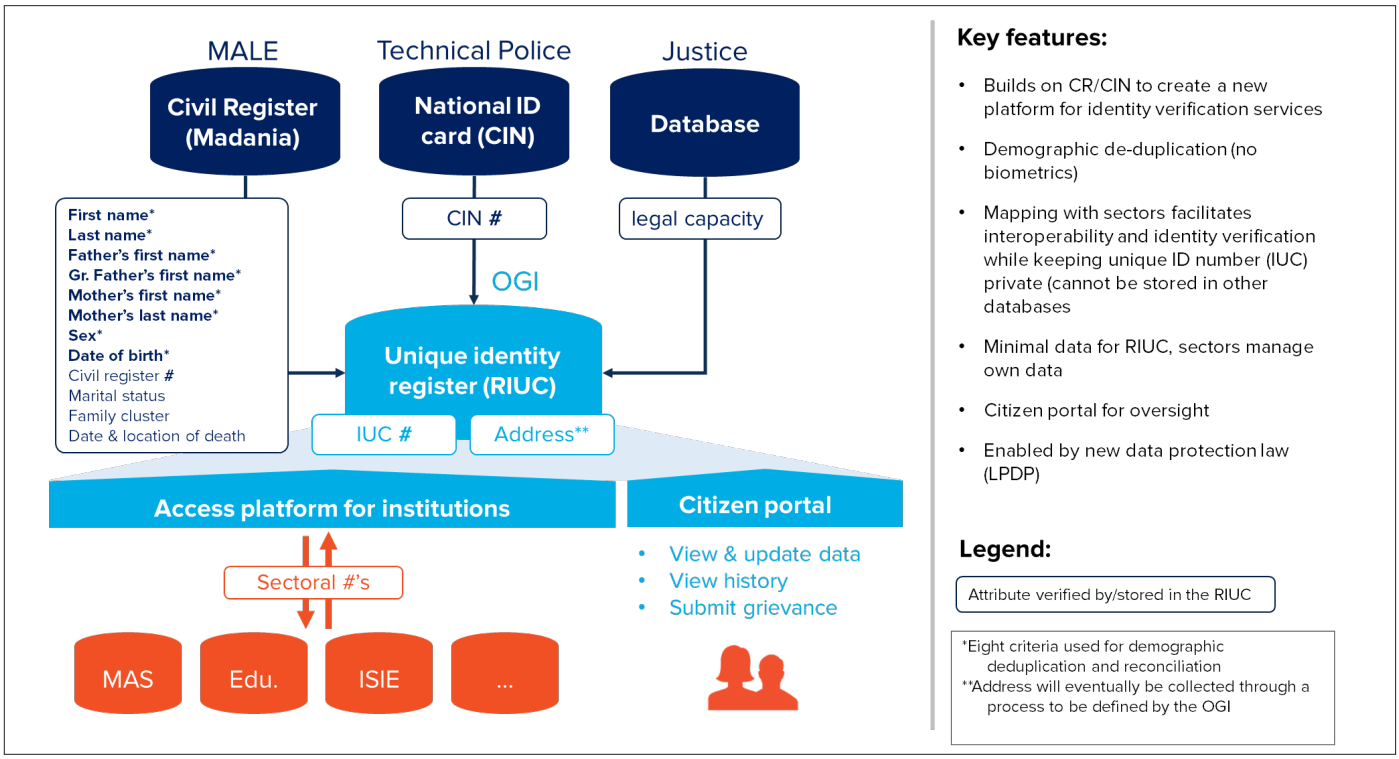
Tunisia has a long history of registration and identification, and most people are able to prove their identity through the country's **two main "foundational ID" systems**: (1) the civil register (CR), which has a birth registration rate of 99 percent, and (2) a national ID card (CIN) held by the majority of citizens aged 18 and over. Despite the broad coverage of these systems and their relative robustness, some issues remain regarding data quality, management of a multilingual database, and full interoperability. Furthermore, neither provide a mechanism for secure, digital authentication for either in-person or online transactions.

In addition to these foundational systems, there are a **number of "functional ID" systems** created for sectoral or ministerial use that provide proof of identity for specific services. The most developed of these are the registers for various contributory and noncontributory social protection and health insurance funds, which have recently implemented a social identifying number (IS) to improve interoperability and record management across the sector. In Tunisia, all functional ID systems rely on the CR or national ID in the sense that they require birth certificates and/or national ID cards as part of the enrollment process and as proof of identity for transactions (for example, collecting a social security payment)—few additional credentials exist.

As part of its ambitious plans for digital transformation—embodied in the national strategic plan (PNS), *Tunisie Digitale 2020*—the government has begun to implement a new ID system to create an "authoritative source" of basic identity information based on a **"unique citizen identifier"** (IUC) (see figure 1). This system will combine data from the civil register and the national ID card, perform demographic—not biometric—deduplication, and assign a unique number to each citizen from birth to death. The IUC register (RIUC) will then function as a dictionary to facilitate and translate identity queries across different sectors, each with their own identifiers that will be mapped to the IUC and stored in the IUC register. Based on the new data protection law, the IUC will be purely a backend system and the number will not be shared with people or other agencies. As a result of this legislation, there will be a continued need for separate sectoral identifiers to link into the IUC system.

Moving forward, there is a high level of interest from different sectors in leveraging the IUC, and the ability of these identifiers and a planned **national interoperability platform** (TunXRoad) to increase the efficiency of administration and improve services for citizens. However, more work needs to be done in terms of the strategic vision and technical implementation of how to best leverage Tunisia's foundational ID systems for sectoral use.

Figure 1. Planned Unique Identity Register (RIUC)



Building a Digital ID Ecosystem for Tunisia: Opportunities, Challenges, and Recommendations

Overall, the government has made significant progress in improving the identification of citizens as part of a broader strategy of digital transformation under the PNS. **Key strengths include** achieving high coverage in the country's foundational ID systems (that is, civil register and a national ID card) as well as specific efforts in priority areas, such as the design and pre-implementation of the IUC, a computerized civil registration system (*Madania*), and the development of a social protection system. In particular, the design of the Tunisian IUC system has a number of privacy-protecting features that—if implemented well—could provide a new model in the region. Furthermore, the government is implementing or planning multiple related projects to develop digital identity infrastructure, showing that there is a clear demand for identification, authentication, and trust services which can serve the needs of various programs and users.

At the same time, **a number of gaps and challenges remain**, including known issues with data quality and a lack of interoperability between systems, limited existing solutions for digital authentication, and some uncertainties around project accountability coordination and governance, and the operationalization of new identity infrastructure in the actual delivery of various programs and services. Therefore, **this report makes the following recommendations** on how to capitalize on its momentum and ensure that its ID systems meet the goals of the government and the Tunisian people:

1. **Establish a multistakeholder committee to synchronize projects and provide a holistic vision for the future of ID in Tunisia**. Although the PNS provides a broad perspective and there are various ongoing projects, there is not yet a clear vision of how all the identity-related projects—for example, the IUC, the social identifier (IS), digital authentication solutions, TunXRoad—will work together in a more coordinated manner. Therefore, it is critical that the government convene a broader

group of stakeholders which will take full stock of ongoing ID and authentication projects and work together to define a more specific medium-to-long term vision related to identification and authentication infrastructure. It is important to note that the stocktaking will review the governance and administration aspects to inform how the institutional structure can be strengthened through a change management process surrounding specific projects (for example, the IUC).

2. **Ensure IUC design will result in a trusted, inclusive, and useful system.** The RIUC is envisaged as a unique identity register that will provide secure verification services to different sectors. For the IUC to play this role, its design must be inclusive (cover the entire population), trusted (reliable, secure, and accountable), and accessible and useful to a variety of users (people and institutions including sectorial ministries). Although much progress has been made, additional technical decisions and planning are needed to ensure that the IUC meets these criteria. Furthermore, maximizing the benefits and use of the IUC hinges on ongoing improvements to the **quality and accuracy** of the civil register (*Madania system*) and the implementation of a **national interoperability framework**—both of which need to be prioritized.

3. **Accelerate development of digital authentication solutions.** Despite a push for digital government and e-services and an existence of a number of authentication-related projects which are currently underway at different stages of development, Tunisia currently lacks universally deployed or adopted digital credentials or platforms to enable secure online and in-person authentication. As already flagged in the first recommendation, more holistic thinking is needed to ensure that planned authentication solutions will: (i) meet the needs of various users and future types of transactions; (ii) be cost effective and interoperable; and (iii) be accessible by the broader population.

4. **Strengthen sectoral information systems and registries while planning for integration with national systems.** Each sector will need to continue improving their databases (for example, beneficiary registries) and developing digitalized, interoperable back-end systems for their existing programs and services in order to eventually connect with or use the national systems (for example, the IUC, digital authentication solutions, TunXRoad). In some cases, such as health and education where a centralized registry of patients and unique sectorial identifier do not already exist, significant investment is needed. In other cases, such as social protection sectors, there has been already significant progress in terms of implementing a beneficiary registry, sectorial identifier, and interoperability framework, and there is now the potential to move forward towards a more integrated system to identify potential beneficiaries of different social programs.

5. **Protect data and privacy by design.** The design of the IUC system already includes certain privacy-enhancing elements (for example, the fact that the number will be private and not stored in other databases), which are enshrined in the Personal Data Protection Law (LPDP), which is currently being debated in the parliament. In order for these designs to be successful, however, stakeholders must work to ensure that these regulations are well understood and implemented, and that complementary data protection and-security-by-design measures are incorporated throughout the IUC system and, more broadly, in other existing and planned identification and authentication systems. In terms of the first concrete step, privacy impacts need to be identified. Consequently, mitigation measures need to be designed to address potential negative impacts identified, and control mechanisms need to be put place when operationalizing these mitigation measures to ensure the protection of personal data in the process of data sharing across agencies.

PART 1. Introduction

1. Motivation for this Study

Tunisia has a long history of registration and identification, and most people are able to prove their legal identity. Tunisia's legal and institutional framework guarantees the right to register and obtain proof of life events, and UNICEF estimates that birth registration coverage is 99 percent. In addition, the national ID card (*Carte d'Identite Nationale*, or CIN) covers a majority of citizens over the age of 18. The Government of Tunisia (GoT) also operates a variety of functional ID systems—including databases, identifying numbers, and cards—to identify the population for specific purposes, including numbers for social programs and health insurance, a tax identification number, passports, driving licenses, and a voter register.

However, while the coverage of these systems is high, none of them can ensure uniqueness and 100 percent coverage of the population, and they suffer from a number of inefficiencies. As a result, many existing programs face common challenges in fully meeting the identification and authentication needs of their beneficiaries. Although databases are digital, the level of integration and interoperability is low. Furthermore, there are often lengthy in-person procedures for people to apply for and prove their identity. Authentication for government-to-person transactions is entirely manual and consists of people giving their ID number (for example, a social insurance number) or presenting their CIN cards for visual inspection. As Tunisia moves toward a more digital economy, there is a strong push to create platforms for online services and transactions in both the public and private sector.

To this end, the GoT is planning or has begun implementing a number of identity-related projects. Notably, this includes the creation of a unique ID number (*Identifiant Unique Citoyen*, or IUC) with the goal of providing lifelong unique identification for all Tunisians and improving the interoperability and integration of identity databases. The IUC—which is in the process of implementation—is intended to underpin the country's digital development agenda (including *Tunisie Digital 2020* and the *Plan National Strategique* or PNS), simplify administration, reduce fraud and forgery, and increase transparency and convenience for users. In order to improve sectoral interoperability, the Ministry of Social Affairs (MAS) has also taken important steps to develop a unified register of beneficiaries to improve the administration and delivery of social protection programs, including the implementation of a social identifier (IS). Additional projects include a national interoperability platform (TunXRoad), a digital benefits card for health, and e-government services that will require some method of digital authentication.

Given that the World Bank has been supporting the GoT with multiple identity-related projects, the motivation of this study was to understand the current state of identification systems in Tunisia as a whole ecosystem across all sectors. The Diagnostic was launched in October 2017; initial findings were shared with participating ministries and departments on July 19, 2018, and informed stakeholder consultations held in September 2018. A draft version of the report also informed the preparation of an e-governance project in Tunisia funded through a World Bank loan. The report was finalized and validated by the government in September 2019, and its contents are current as of that date.

Overall, the report finds that while significant progress has been made in terms of information system development and the rollout of the IUC and IS, the next step toward maximizing the potential of these tools is to develop concrete plans for their continued development and improvements to the functionality of the ID ecosystem as a whole. In particular, more work is needed to: (1) finalize the implementation of the IUC

and its governance arrangements and ensure that projects to improve the accuracy and reliability of data are complete; (2) develop a concrete plan for how the IUC will be leveraged by different systems (including the mapping of sectoral identifiers to the IUC and the potential for the IUC to facilitate interoperability of identities between sectors); (3) build secure system(s) for online and in-person authentication to enable e-services and improve efficiency; and (4) improve the coordination of stakeholders and harmonization of the various identity-related projects currently underway.

Box 1. Key Identity-Related Terms

An identification or **ID system** consists of t*he databases, processes, technology, credentials, and legal frameworks involved in the capture, management, and use of personal identity data for a general or specific purpose*. The main technical infrastructure of an ID system are typically **databases** (or registers) of identity data and the **credentials** issued by the system and used by individuals to prove their identity or particular attributes, such as cards, PINs, or mobile apps. In addition, ID systems include a variety of **platforms** through which third parties can use these databases or credentials to verify or authenticate identities, such as interoperability layers that facilitate data exchange, queries, and identity-related transactions.

In general, ID systems can be categorized into those that are "foundational" and those that are "functional." **Foundational ID systems** are created with the goal of providing *general identification and credentials for a variety of purposes* and typically include civil registers, national ID cards, population registers, and so on. In contrast, **functional ID systems** are designed primarily *to provide identification for a specific purpose or sector* such as voter registers, tax ID numbers, social protection registers, driving licenses, and so on. Functional ID systems typically maintain databases with attributes specific to their purpose that are used for authorization—such as poverty scores and household assets for social protection, or annual income for tax systems—and may or may not issue their own credentials. Together, the *collection* of foundational and functional ID systems within a country make up the **identity ecosystem**.

After a brief explanation of the role of identification for development, the remainder of this report is organized as follows: Part 2 provides an update on the status of identity projects and their progress since the benchmarking study commissioned by the GoT in 2015 that led to the development of the IUC. It gives an overview of existing databases and credentials, as well as ongoing projects and issues with implementation. Part 3 then provides a summary of the main achievements, as well as ongoing challenges and uncertainties regarding identification in Tunisia across these various systems and projects, and then provides recommendations for addressing these issues in the future.

2. Identification for Development

Inclusive and trusted identification (ID) systems are crucial tools for achieving sustainable development. For this reason, ensuring that everyone has access to ID is the explicit objective of Sustainable Development Goal (SDG) Target 16.9—to "provide legal identity for all, including birth registration" by 2030. Furthermore, identification is also a key enabler of progress towards many other SDG targets, such as financial and economic inclusion, social protection, healthcare and education for all, gender equality, and safe and orderly migration by:

- Empowering individuals and enhancing their access to rights, services, and the formal economy
- Strengthening the transparency, efficiency, and effectiveness of governance and service delivery
- Supporting private sector development
- Growing the digital economy
- Supporting regional and global integration

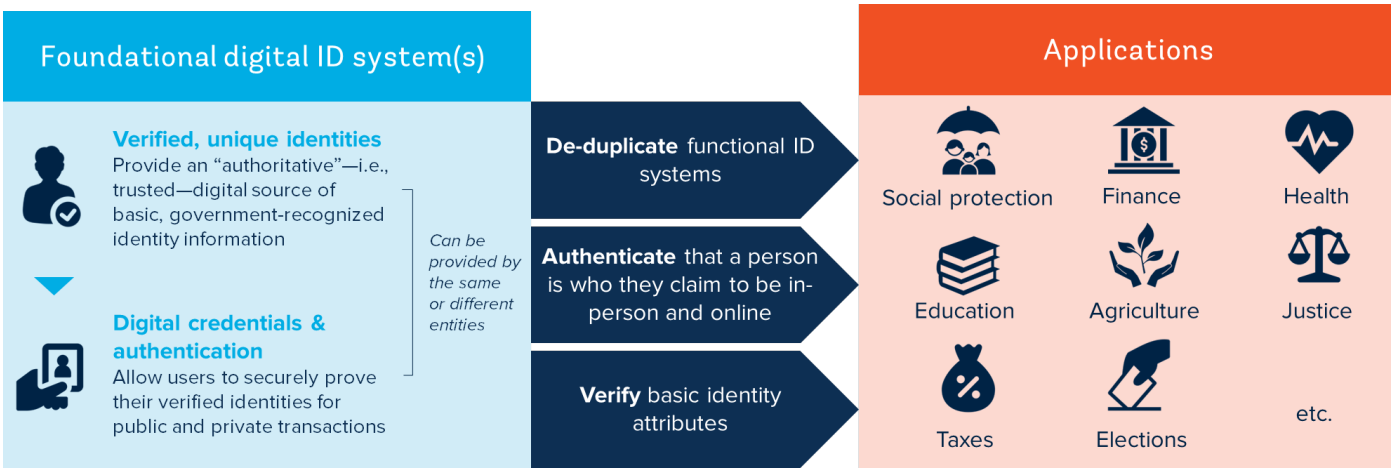
As shown in Figure 2, foundational ID systems (see Box 1 for definition) can serve two important functions within the identity ecosystem and across a variety of sectors: [1]

1. **Authoritative source of basic identity information.** By creating a register of unique, verified identities, a foundational ID system can provide the basis for secure identity verification for government and private-sector users. In any country, having a trusted source of basic identity information is vital to the integrity of the identity proofing process for the government's functional ID systems (for example, social protection, elections, and so on) and for private-sector ID providers and relying parties (for example, financial institutions or mobile network operators conducting know your customer (KYC) processes). Beyond the verification of identity attributes themselves, a foundational system with unique identity records can also help deduplicate functional systems—for example, a cash transfer register or public payroll—reducing opportunities for fraud and the need for redundant data collection by the foundational system.

2. **Digital credentials and authentication.** In addition to establishing an authoritative source of identity information that can be leveraged by other systems, foundational ID systems can also provide credentials that allow people to authenticate their identities for a wide variety of purposes and sectors. As with verification, authentication can be a shared service provided to a variety of public and private sector users. When built as a platform that allows users to leverage the ID systems' credentials and authentication mechanisms rather that building their own—for example, through federation or mutual recognition frameworks—this can help reduce costs for government agencies and private companies.

1 For more on the potential benefits and cost savings of foundational ID systems, see World Bank. 2019. ID4D Practitioner's Guide. Identification for Development. Washington, DC: World Bank Group. http://id4d.worldbank.org/guide; World Bank. 2018. Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints. Washington, DC: World Bank; and World Bank. 2018. Private Sector Economic Impacts from Identification Systems. Washington, DC: World Bank, both available at http://id4d.worldbank.org/research.

Figure 2. Identity as a Platform for Development



Importantly, while foundational ID systems provide identity verification and authentication services that can streamline administrative processes and increase the security of transactions across sectors, they do not replace the need for strong sectoral registers and information systems. To meet international standards on data privacy and protection, foundational ID systems should contain only the *minimum data necessary* to establish and verify a person's basic identity and uniqueness and provide identity verification and/or authentication. In parallel, different sectors maintain and operate their own functional registers with relevant, sector-specific information (for example, health records, student records, social benefits information, and so on). This separation of purposes helps protect personal data while allowing a wide variety of public and private sector institutions to leverage the identity verification and/or authentication services provided by foundational ID systems.

In the past, most foundational (and functional) ID systems were paper based and operated or managed entirely by governments, but digital ID has broken this mold. With the move toward digital technology throughout the identity lifecycle, new models are emerging of partnerships or trust frameworks between governments and the private sector to provide digital authentication solutions that are recognized by the government for official online transactions (i.e., e-government services). Typically, these systems rely on existing foundational ID systems as authoritative sources of information and then provide additional digital authentication and verification services through new channels (for example, mobile ID applications, (see Box 2).

Box 2. Basics of Authentication

Authentication is the process of verifying that a person is who they say they are—that is, that the person who is claiming or "asserting" a particular identity is the same person who enrolled in the first place. This process involves checking one or multiple authentication credentials/factors against one another to see if they match the claimed identity. Common authentication factors include:

Something a person...

Digital authentication—which uses electronic credentials and processes—can be used to increase the security of ***in-person*** transactions (for example, using a smartcard and PIN at the hospital office). Unlike analog authentication processes, such as examining the photo on someone's ID card, digital authentication can provide a much higher **level of assurance** (trust) that the person is who they claim to be. Furthermore, along with digital certificates and signatures, digital authentication enables secure ***online*** transactions, such as e-services and mobile money.

Different types of transactions require different **levels of assurance**, as determined by the robustness of the identity proofing process—that is, vetting identity information and supporting documents—during enrollment, as well as the types of credentials issued and the technology used for authentication. For example, a self-created email address and password combination provides a lower-level of assurance than a smartcard-based national ID that was issued after in-person identity proofing, and which uses public key infrastructure (PKI) encryption and a PIN for authentication.

In order to maximize their developmental impact and minimize risks to privacy and exclusion, ID systems should—at a minimum—meet the *ten Principles on Identification for Sustainable Development*, shown in Figure 3. These *Principles* have now been endorsed by over 25 international organizations, donors, NGOs, and private sector associations.

Figure 3. Principles on Identification for Sustainable Development

Principles	
Inclusion: Universal Coverage and Accessibility	1. Ensuring universal coverage for individuals from birth to death, free from discrimination. 2. Removing barriers to access and usage and disparities in the availability of information and technology.
Design: Robust, Secure, Responsive And Sustainable	3. Establishing a robust—unique, secure, and accurate—identity. 4. Creating a platform that is interoperable and responsive to the needs of various users. 5. Using open standards and ensuring vendor and technology neutrality. 6. Protecting user privacy and control through system design. 7. Planning for financial and operational sustainability without compromising accessibility.
Governance: Building Trust By Protecting Privacy And User Rights	8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. 9. Establishing clear institutional mandates and accountability. 10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.
Source: http://id4d.worldbank.org/principles	

PART 2. Identification in Tunisia: Assets and Gaps

This section provides an overview of the main ID systems in Tunisia and assesses their strengths and weaknesses with regard to coverage, technology, interoperability, and governance. It begins with an overview of the ecosystem as a whole, along with the main identity stakeholders, and then discusses specific foundational and functional ID systems (for a review of these terms, see the Introduction).

1. Overview of Tunisian ID Ecosystem

The GoT operates a number of ID systems that provide a high level of coverage within the population. This includes two "foundational ID" systems used to provide general identification for a wide variety of purposes and transactions: **(1) a civil register (CR)**, managed by the Ministry of Local Affairs (MALE) and **(2) a national ID card (CIN)**, issued by the technical police (*police technique*) under the Ministry of Interior. Together, these systems provide offline proof of legal identity for the vast majority of people in Tunisia. The government is also currently in the **process of implementing a foundational register of unique identities** (the RIUC or *Registre de l'Identifiant Unique du Citoyen*) based on the CR and the CIN databases, which will serve as an authoritative source of identity information and facilitate identity queries and data exchange across government agencies.

In addition, there are a **number of "functional ID"** systems provided for sectoral use by different ministries, including for social protection and taxation. In particular, the Ministry of Social Affairs (MAS) and its sub-agencies that manage social protection funds are important stakeholders in Tunisia's identity ecosystem, as together they operate ID systems that cover the majority of the population. Other sectors, such as health, do not currently have centralized databases of beneficiaries, or standardized credentials/identifiers. Major systems, along with their providing agencies, are summarized in Table 1.

Table 1. Overview of Main ID Systems and Registers

	System	Responsible Agency	Credentials and Identifiers	Coverage
Foundational ID	Civil register (CR)	Local governments, centralized in *Madania* database run by MALE	Birth, marriage, divorce and death certificates, family book	99 percent of the population
	National ID Card (CIN)	Police, under the Ministry of Interior	Current: CIN #, card Planned: eCIN smartcard	Coverage of adults about 90% (estimation)

	In progress: Unique citizen identifier registry (RIUC)	Currently MALE in partnership with the of Ministry of Technology (MTCEN), and implementation by the National Informatics Center (CNI), later to be run by a separate management body (OGI) under the MALE	Unique citizen identifier (IUC) – will be a private, back-end key not used during authentication	15 million (including living people and those deceased for less than 30 years; the register is operational but the whole system is still being implemented)
Functional ID	Social protection and health	The Social Research and Study Center (CRES) within the Ministry of Social Affairs (MAS) and with social security funds (CNSS and CNRPS)	Social ID number (IS) [In parallel, social security funds use their own identifying numbers for beneficiaries, which preceded the implementation of the IS]	10.2 million, however some are deceased and duplicated (February 2019)
		National health insurance fund (CNAM)	Digital card	Distribution started in April 2019 (not yet used)[a]
	Taxes	General Directorate of Taxes *(Direction generale des impots)*	Tax number	~3 million (c. 2015)
	Voter register	Electoral commission (ISIE)	None	5.4 million (c. May 2018)[b]
	Education	Ministry of Education and National Center for Education Technologies (CNTE)	Student identifier	~2 million (c. 2019)
Note: a. http://www.cnam.nat.tn/doc/upload/fr_com_carte.pdf; b. High Independent Authority for Elections (ISIE), http://www.isie.tn/electeurs/.				

In addition to the identity providers detailed in Table 1, there are a number of **other important stakeholders** in Tunisia's identity ecosystem, described below in Table 2. This includes the Ministry of Technology (MTCEN), which in addition to providing leadership on the IUC and other projects, houses the National Informatics Center (CNI) that is responsible for the technical development of the RIUC and the CR systems. The Electronic Administration Unit (UAE) within the Ministry of Public Administration is responsible for diagnostics, policy and legal development, and monitoring and evaluation of projects implemented in the e-government sector. The National Authority for the Protection of Personal Data (INPDP) also plays an important role in the oversight of identity programs, and in the drafting of new legislation on data protection and privacy.

Finally, the National Agency of Electronic Certification (TUNTRUST/ANCE) operates a public key infrastructure (PKI) to ensure a trusted digital environment to underpin development of the digital economy. TUNTRUST offers digital certification and signature services[2] and has developed a Visible Electronic Cachet for the securing of administrative documents via an electronic signature made visible through a QR Code (two-dimensional bar code).[3] Currently, TUNTRUST is developing multiple digital authentication solutions but these have not been widely deployed or adopted.

2 Currently, these electronic seals are used for the following e-government services: (1) Tuneps (online public procurement), (2) online tax declarations (e-jebaya), (3) online employer declaration (CNSS, CNRPS), (4) foreign commerce (TTN), and (5) electronic invoice project.

3 This service is currently used for baccalaureate and ninth year certificates, extracts from the National Register of Companies, and university degrees.

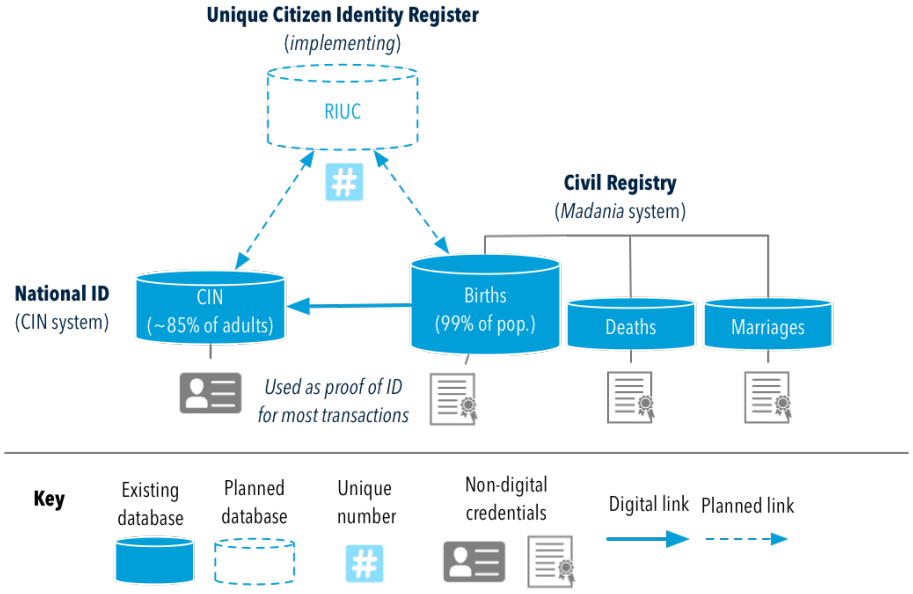
Table 2. Other Important Government Stakeholders in the Identity Ecosystem

ENTITY	ROLE
Ministry of Technology (MTCEN)	Technical oversight of ICT and communications work in Tunisia, including technical oversight of the IUC project and national interoperability framework
National Informatics Center (CNI)	Technical implementation of CR system (Madania) and the IUC
Electronic Administration Unit (UAE) of the Ministry of Public Administration	Unit responsible for diagnostics, policy and legal development, integration of ICT reforms with the administrative reform agenda, monitoring and evaluation of policy implementation in the area of e-government, including e-services, ID, and the Smart Gov strategy
National Agency of Electronic Certification (TUNTRUST/ANCE)	Provides digital certificates and e-signatures for some services
National Authority for the Protection of Personal Data (INPDP)	Independent, legally constituted, and financially autonomous body tasked with the monitoring and oversight of entities that process personal data, including identity providers

2. Foundational ID Systems

This section covers the **two main foundational ID systems in Tunisia—the civil register and CIN—**in detail. It also describes the **unique citizen identity register (RIUC)**, which is part of the PNS (see Figure 4). The RIUC is expected to modernize the country's ID systems by facilitating identity verification services and interoperability between various sectoral databases, however, the project is still in early implementation, with plans for full deployment by 2021.

Figure 4. Foundational ID Systems in Tunisia



Civil Registration (CR)

Tunisia has a strong civil registration system, which in its modern form dates back to the early twentieth century. The law on civil registry was adopted in 1957 after independence, making the registration of birth and deaths compulsory and establishing the right to obtain proof of vital events.[4] Civil registration—including birth registration, death registration, and marriage contracts—is conducted by local governments. This primarily includes the country's 350 municipalities (communes), although other local administrative bodies (delegations) also undertook these activities in rural areas until 2018.[5]

In order to complete the birth registration process, parents are required to visit the local CR office at the municipal headquarters and present documentation of the birth (for example, a medical certificate), proof of identity of the mother and father (a CIN card), and a signature. Registration is free of cost and must be done within 10 days of birth or it is considered a late registration and must then be completed in court (at

4 See the text of the law at https://www.jurisitetunisie.com/tunisie/codes/csp/civil1000.htm.
5 Previously, there were 264 municipalities that only covered urban areas within the country. Residents of rural areas would instead go to administrative officers within their delegation (Mouatamdeya) for services. Beginning in 2016, however, new municipalities were created (and old municipalities were expanded) to continuously cover the territory, so the entire population is now under the jurisdiction of a municipality and its elected council.

the Tribunal de Première Instance).[6] Death registration follows a similar process and must be completed within three days of death. Overall, UNICEF estimates a birth registration of 99 percent (see Table 3).

Table 3. Coverage of Civil Registration

Civil Registry	Enrollment
Target population	All residents of Tunisia and Tunisian citizens living abroad
Target population size	11.4 million people in Tunisia (2016)
Mandatory?	Yes, within 10 days of birth (for residents)
Total coverage[a]	Acts recorded (living and deceased persons) as of 2018: 18.53 million births 4.14 million deaths 3.8 million marriages
Birth registration rate[b]	99 percent
Source: a. MALE (2019); b. ID4D Global Dataset, 2018 (original birth registration data is from UNICEF, circa 2016).	

CR Database and Integration

Civil events are recorded at the municipal level in physical ledgers (registers). Data on birth, deaths, and marriages are then manually entered into the civil registry information system, called *Madania* ("civil" in Arabic), by local officials. The system was first deployed in 1992 by the CNI in the municipality of Tunis, and then rolled out nationally beginning in 2004.[7] As of 2015, it was accessible from nearly 481 sites (all municipalities plus regional and commercial sites) and 1,300 workstations across the country and utilized by approximately 1,500 people.

Before the digitization of the CR and the development of the *Madania* system in both French and Arabic, people would have to travel to the place where the civil act was originally registered (for example, their birth location) to request copies of certificates based on paper ledgers. With the *Madania* system in place, they can go to any municipal office and request copies of documents or correct errors. In the case of updates, these changes are reported to the municipality where the event occurred to be amended in the physical register and are then uploaded to the database.

Notably, records of different events (births, deaths, and marriages) are maintained separately within the *Madania* system without systematic links between them—for this reason, the system does not serve the function of a population register with a unique record for every individual. However, an ongoing project to improve data quality (see below) will put in place more systematic checks and controls between the databases.

6 http://www.collectiviteslocales.gov.tn/etat-civil/.
7 https://www.webmanagercenter.com/2005/05/16/11728/madania-2-un-projet-de-e-gouvernment/.

Table 4. Attributes Stored in the Madania Birth Registration Database

Type	Attributes	Collection
Biographic	1. First name 2. Last name 3. Date of birth 4. Place of birth 5. Sex 6. Father's name chain (father's first name + grandfather's first name) 7. Father's birth date 8. Father's birth location 9. Father's profession 10. Father's nationality 11. Mother's name chain (mother's first name + grandfather's first name + mother's last name) 12. Mother's birth date 13. Mother's birth location 14. Mother's profession 15. Mother's nationality 16. Name, age, profession of declarer	Entered into a paper register, then manually entered into Madania database.
Metadata	1. Date of declaration 2. First name of officer professing application 3. Last name of officer	
Biometric	none	N/A

Currently, there are few automated links between *Madania* and other systems (see Table 5). In most cases, authorized ministries or other entities can request a copy of certain information, which is sent in digital format via physical media. However, the government is in the process of implementing services to allow for easier, automated queries of the *Madania* system.

For example, the "e-madhmoun" system allows for the exchange of birth extracts between government agencies via a web-based platform operated by the CNI. The first pilot of this system was with the Ministry of Education (see section below on functional ID systems), and implementations are currently being developed to cover the social sector (MAS), and the Ministry of Employment, Professional Development, and Higher Education.

Table 5. Data Storage and Transfer for Madania

Civil Registry	CR (Madania) Database
Database architecture	Three separate (and unconnected) databases for births, deaths, and marriages/divorces, hierarchical: local → regional → central
Databases with which system exchanges information	Exchanges data with: • Ministry of Education (via e-madhmoun web platform) • CNRPS (as needed) via a text file and FTP server (since March 2019 via the e-madhmoun system) • CNSS (as needed) via a text file and FTP server (since March 2019 via the e-madhmoun system) • ISIE for elections • National Institute of Statistics (INS) for vital statistics Synchronization occurs in batches at night, during which the database is unavailable.
Database technology	SQL server, 18GO
Backup and disaster recovery	Backup server with DSI in Ministry of Interior

A key challenge in cleaning the CR database and integrating it with other systems has been the format in which names are recorded in Arabic and French. Currently, the family names in Arabic, including the father's and grandfather's names, are captured as a single "chain" field. Given the structure of Arabic names—both first names and family names are frequently compound words—the chaining makes it difficult to reconcile with other data sources. In addition, there is often significant variation in how Arabic names are transliterated and captured in the Latin alphabet.

In addition to language issues, there are some other problems with data accuracy in the system, such as the double entry of births. As of 2015, some 300 thousand double declarations of births had been detected. In addition, late registrations, as well as vital events of Tunisians abroad, only recorded every six months, cause a delay in updating the system. Furthermore, because records of births, deaths, and marriages are maintained in different databases, there are opportunities for errors and inconsistent identity data across the three records systems. Finally, the *Madania* reference number is quite long (20 digits) and does not include checksums, leading to frequent transcription errors.

Certificates and Numbers

The primary credentials issued by the CR include birth, death, and marriage certificates and reference numbers (used to locate the act), along with a family book. Birth certificate, extracts, and family books are commonly used as proof of identity and civil status for various purposes, often in combination with the CIN (for adults). All certificates are paper based and include reference numbers encoded with place and date of issue (see Figure 5 and Table 6). However, although the number of the civil act is frequently recorded in other databases (for example, in the social insurance funds), certain checks to verify a person's birth are done by matching eight primary attributes—first name, last name, date of birth, gender, father's first name, grandfather's first name, mother's first name, and mother's last name—against the *Madania* system, rather than using the number itself.

Figure 5. Structure of the CR (Madania) Reference Number

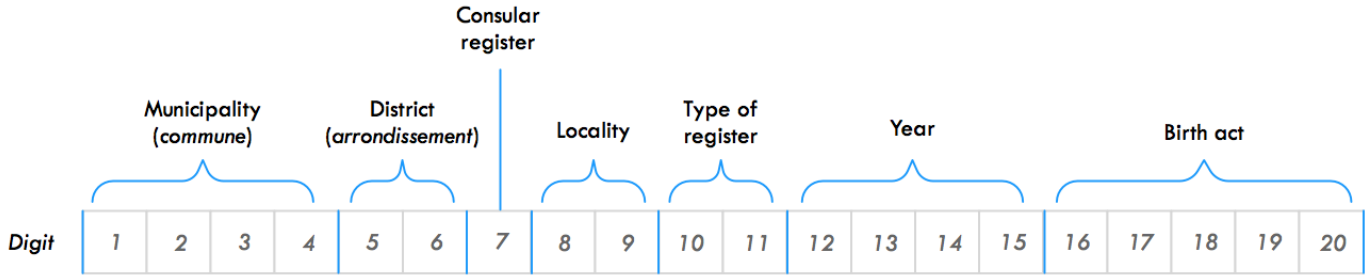
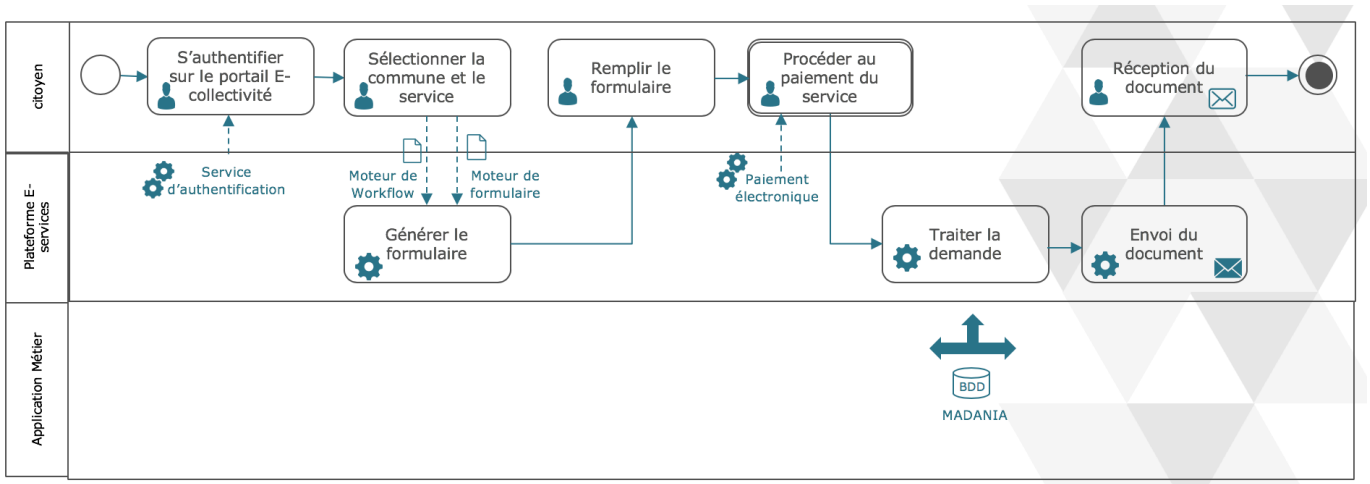


Table 6. Birth Certificates and Extracts (Extraits de naissance)

Civil Registry	Birth Certificate And Extract
When issued	At birth registration, additional copies (extracts) can be requested later
Cost	First copy free, TD 0.5 ($0.18) for extra copies
Expiration	Never, however for certain services (e.g., obtaining a CIN card) the extract must be recent (typically less than three months old)
Type and format of reference number	20 digits, coded with: • Municipality (*commune*) [4 digits] • District/neighborhood (*arrondissement*) [2 digits] • Consular register [1 digit] • Locality [2 digits] • Type of register [2 digits] • Year [4 digits] • Birth registration act [5 digits—local sequential series that starts from 0 each new year]
Numbers of deceased are recycled?	No, because numbers include year of issue
Material	Paper certificates
Machine readability	*Current:* None *Planned:* Certificates/extracts will be printed with QR codes
Time to issue	Issued on the spot if application is complete
Method of collection	In person (can be collected by a parent, child, or spouse of the person), or via post (must be present and have ID to collect). It is also possible to make the request online and collect in person via https://www.etatcivil.gov.tn/Madania/web/indexfr (partially operational since 2018).

Because recent copies of the birth extract are commonly required for administrative processes, people often need to obtain updated versions of these documents. Previously, this required an in-person visit to a municipal office. Beginning in 2018, however, the MALE—in cooperation with MTCEN, CNI, and the Tunisian Post—implemented a service that allowed people to request copies of their birth certificate (extrait de naissance) online via using their CIN number. After completing the application and payment, paper copies of certificates are sent via post to the applicant's home in Tunisia or abroad and delivered after checking their CNI. However, while the service can save people a trip to the municipal administration—which is particularly convenient for Tunisians abroad—in the longer term, the goal is to reduce the number of services that require people to present their birth certificate by implementing automated back-end requests to verify information in the civil register (for example, as with e-madhmoun and via the RIUC as described in Figure 6).

Figure 6. Planned e-Services request for Birth Certificates



Source: MALE.

Plans for Reforming the Madania System

The MALE, MTCEN, and CNI have developed a strategy to upgrade the Madania system that will address some of the data quality and integration issues described above. Overall, the goal is not only to upgrade the performance of the current system, but to turn Madania into a modern platform that serves the business needs of multiple stakeholders. Specific goals include (but are not limited to):

- Facilitating the interoperability of the Madania system with the IUC, CIN, CNSS, CNRPS, and potentially other ministries and public bodies (for example, Ministry of Health, Ministry of Defense, Ministry of Education, Ministry of Higher Education, national statistics agency (INS)
- Moving to a paperless system that reduces the physical contact necessary between citizens and the administration
- Improving the quality and accuracy of data, including, by "dechaining" of family names (for example, father's and grandfather's first names) and linking different CR records (birth, marriages/divorces, and deaths)
- Determination of family clusters—that is, linking family members in the database
- Providing relevant public bodies (for example, hospitals, Ministry of Education, INS) with vital statistics information
- Encouraging secure electronic exchanges between CR offices at the municipal level
- Improve security and confidentiality of data (including through encryption, strong authentication
- Moving to a service-oriented architecture, open technologies, and independence from proprietary technologies
- Develop an interoperability platform, e-services, and mobile services

According to current plans, the system will be developed over the course of 2020 and deployed during 2021.

National ID (CIN)[8]

The national ID card (Carte d'identite nationale, or CIN) is the other foundational ID system in Tunisia, and is estimated to cover a large majority of the population of adult citizens. Cards are issued beginning at 18 years of age[9] and are used as proof of identity for nearly all transactions (see Table 7).

Table 7. CIN Coverage

National ID	CIN
Target population	Citizens, mandatory at age 18, can be obtained earlier
Target population size (18+)	8.3 million (c. 2018)[a]
Target population covered	Coverage of adults around 90% [b]

Note:

a. ID4D Global Dataset, available at http://id4d.worldbank.org/global-dataset;

b. Precise numbers pending inputs from the Ministry of Interior. According to some news sources, the coverage is around 7 million (approximately 84 percent coverage of adults 18+), while according to others only some 300,000 adults do not have the CIN. See, for example, https://www.huffpostmaghreb.com/2018/01/03/carte-didentite-biometriq_n_18926246.html and https://www.espacemanager.com/chafik-sarsar-300-mille-tunisiens-nont-pas-de-cartes-didentite.html.

The system is managed by the *Police Technique* (Technical Police) under the Ministry of Interior, and Tunisians apply for and renew their ID cards at local police stations or national guard offices in their area of residence. In order to apply for a CIN (see table 9), a person must provide a birth extract issued within the last three months (see above), certification of Tunisian nationality, certification of residence, certification of employment or student status, certification of blood type (optional), an inked thumbprint, and three photos. After completing an application, police should issue a card within 15 days.[10] The initial application for a card costs TD 3 (about $1), while replacements for lost or stolen cards cost TD 25 (about $9).[11]

Table 8. Administration of CIN

National ID	CIN
ID provider	Technical Police, Ministry of Interior
Offices and responsibilities	• Local police stations and national guard offices: process applications • 31 regional offices: manual data entry, CIN number issuance, card printing • Central office: data validation and archives, overall management

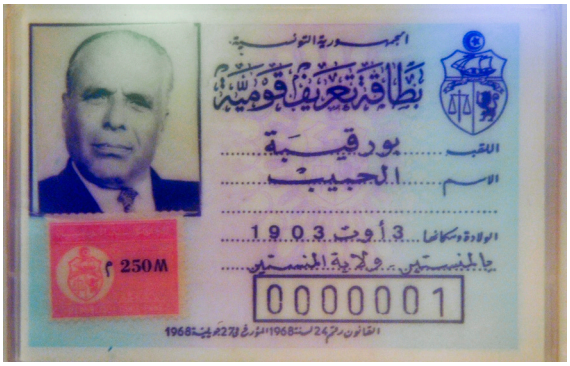
CIN Card

The current version of the CIN is a basic plastic card with a machine-readable barcode that has been issued since 1993 (see Figure 7), replacing the previously issued laminated paper cards (see Figure 8). As of 2014, the older cards were no longer valid.[12] However, about 350,000 paper cards remained in circulation in 2015. In recent years, about 700,000 new or replacement CINs have been issued each year, and some 21 million new and replacement cards were issued between 1993 and 2015[13] for a population of about 11.5 million people. The card is not electronic and therefore authentication procedures using the card involve only a manual check.

8 Note: this section requires validation from the Ministry of Interior/Technical Police.
9 Cards can be exceptionally provided to those under 18 years, which requires extra documentation from the legal guardian, including the reason for needing the card. See http://services.interieur.gov.tn/wap/fr/docs/demarches/01.html.
10 http://services.interieur.gov.tn/wap/fr/docs/demarches/01.html.
11 https://directinfo.webmanagercenter.com/2012/12/28/tunisie-la-cin-a-25-dt-et-le-passeport-a-150-dt/.
12 http://mag14.com/actuel/35-societe/705-tunisie-precisions-sur-le-nouvellement-des-cartes-didentite.html.
13 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#.

Figure 7. New CIN (Post-1993)

Figure 8. Old CNI Issued to Tunisia's First President, Habib Bourguiba



Source: Citizen59 (CC BY-SA 3.0)

Table 9. CIN Card and Number

National ID	CIN
First issued	1993
When issued and to whom	Adult citizens, 18+
Expiration	None
Material	Plastic
Machine readability	Barcode
Human-readable attributes	Last name, first name, father's first name, grandfather's first name, mother's first and last name, date of birth, residence, profession, address, date CIN issued, image of thumbprint, CIN number and control digits
Machine-readable attributes	Barcode contains number of the card
CIN number	8 sequential numbers, with different ranges in different regions (if a region runs out, ranges are transferred from another)
Encryption	None
Credential personalization	Regional offices
Application process	In person
Method of collection	In person
Time to issue	The police reportedly take about15 days to process an application; however, a person is likely to spend at least two weeks obtaining the documentation (e.g., certificate of residence, certificate of nationality, etc.) needed to apply for the CIN. So, it is likely that the entire process from the perspective of the citizen takes an average of one month.
Note: http://www.sicad.gov.tn/Fr/Renouvellement-de-la-carte-didentite-par-une-carte-didentite-nationale_57_3_D1310.	

CIN Database and Integration

During the registration process, paper application forms in Arabic and substantiating documents are collected at the local level and then sent to regional offices (see Table 10). There, biographic information is entered into the database and translated into French, and biometric data are entered (an inked fingerprint and photo). After the CIN number is issued, the data and supporting documents are sent to the central level for reconciliation and storage. After validation of the data, cards are then printed at the regional level.

Table 10. Attributes and Required Documents for CIN[14]

CIN Requirements	Type	Collection	Validation	Storage
Supporting documents	Certificates of birth, nationality, residence, occupation, and blood type (optional); as relevant certificates of marriage or death of spouse if widowed	Paper forms collected	Unknown	Paper records stored in central archives
Biographic attributes (captured in Arabic, translated to French)	Last name, first name, father's name, grandfather's name, date and location of birth, mother's first and last name, gender, family status (single, married, widowed), first and last name of spouse, occupation, current address, blood type (optional) and whether blood donor	Paper application, entered into computer manually	Based on supporting documents	Central biographic database
Biometrics attributes	3 copies of a photograph, inked fingerprint(s), physical signature	Application form, then scanned	Unknown	Central database for biometric images

Data is not deduplicated during renewal, and so it is possible for one person to have multiple CIN cards/numbers, and in some cases multiple people can have the same CIN number. In 2015, it was estimated that there were around 2,500 cases of double cards. In addition, a number of data fields—including address and occupation—are frequently out of date.

Table 11. Data Storage and Transfer for CIN

National ID	CIN
Database architecture	Two databases: (1) biographic information (including data and the card and other data (e.g., the first and last name of the spouse if the person is married), (2) biometric information (scanned images of fingerprints and photos)
Databases with which system exchanges information	**ISIE:** Ahead of elections, CIN gives a list of citizens to the electoral commission **Madania**: Upon request, the CR provides information on a person's civil status and/or death, which involves the physical exchange of a text file
Database technology	**Biographic:** internally developed under Cobol, uses VSE-CICS operating system and VSAM file management **Biometric:** turnkey solution
Backup and disaster recovery centers	Backup for biometric data on a server of the General Directorate of Informatics (DGI)

14 This information is believed to be accurate but has not been confirmed by the Ministry of Interior.

Plans for the eCIN

The Ministry of Interior (MOI) has been developing plans to issue a new biometric smartcard version of the CIN, called the eCIN. The initial proposal included a card with a microchip that would contain a photograph and the right thumbprint of the card holder, which could only be accessible by the police and national guard agents responsible for identity verification. The card and/or chip would also contain data similar to that on the current CIN, including names and surnames of the card holder, their parents, paternal grandfather, the address and CIN number, as well as optional data including the name and surname of a spouse, blood type, and whether the person is an organ donor. The cost of the project was reported to be some TD 40 million ($14.6 million).

In 2016, a draft organic law was introduced to the National Assembly (l'ARP) amending the previous legislation governing the CIN (Law No. 9327 of March 22, 1993) to facilitate the eCIN project. However, the draft was withdrawn in early 2018 owing to concerns regarding privacy. Although the National Authority for the Protection of Personal Data (INPDP) has given its support for biometric authentication via a smartcard chip, it has expressed concern over the security risks associated with the development of a centralized biometric database. In addition, the INPDP and civil society activists have raised concerns over the fact that data stored in encrypted format on the chip would only be accessible by the police, breaching the citizen's right to oversight and transparency over who has access to their information.[15] As of late 2019, the MOI still plans to introduce revised legislation for an eCIN but no date or formal plans have been announced.

Plans for a Unique Citizen Identifier

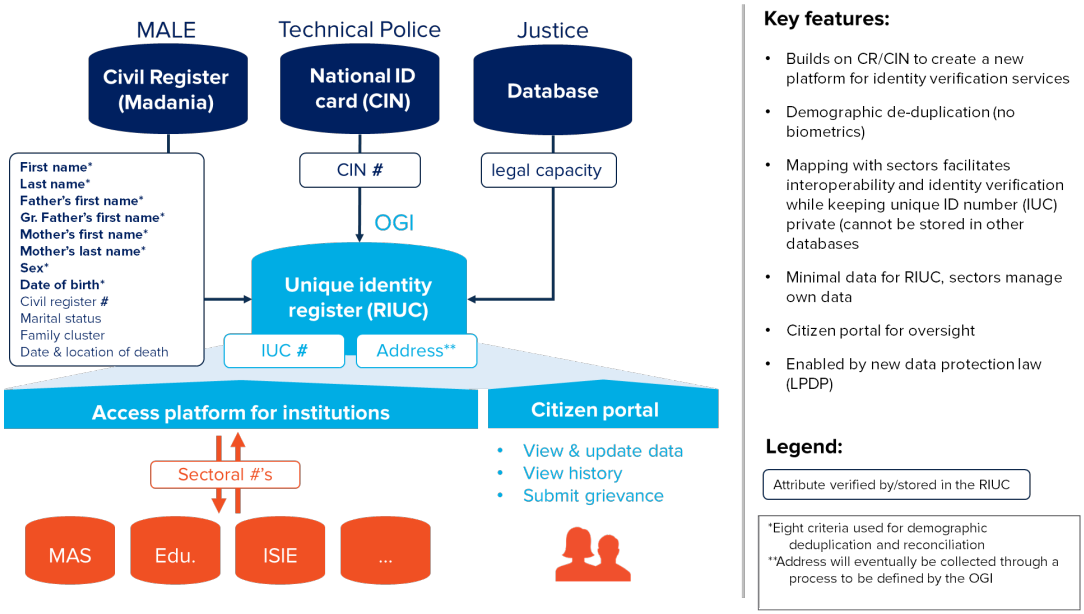
The e-government component of the National Strategic Plan (PNS) *Tunisie Digitale* 2020 calls for the transformation of public administration through the adoption of digital technology that will increase efficiency and transparency for citizens and businesses. This goal was motivated by: (1) the existence of multiple sectoral identifiers and heterogeneous IT infrastructure that limit data exchange between departments; (2) the inaccuracy of identity data in both the foundational and functional systems; and (3) the need to improve administrative procedures and streamline public services delivered to citizens.

In order to further these goals, the PNS called for the development of a unique identifier for citizens—an *identifiant unique citoyen* (IUC)—together with the development of e-services and a national interoperability framework. Planning for the IUC began in 2015 with an initial study conducted on behalf of the Ministry of Technology (MTCEN), which helped develop the preliminary plan for the IUC. A steering committee of stakeholders was formed, and in 2017, the MALE (the project owner), MTCEN, and INPDP signed a memorandum of understanding (MoU) regarding the project roles and governance model. Since then, these three organizations, along with the CNI, have continued to make progress in defining the technical design and implementation plans for the IUC.

As of 2019, the current vision is to create a national reference system—that is, a register and dictionary—that represents an authoritative source of information regarding a person's identity and can be used to facilitate data exchange across the public sector. The system will validate basic identity attributes for all citizens by pulling from the CIN and CR systems, issue an IUC number, and store this information in a **Unique Citizen Identifier Registry** (*Registre de l'Identifiant Unique du Citoyen* or **RIUC**) system. In addition, the system will include platforms for public administrators to query the database, and a citizen access portal for oversight of their data (see Figure 9).

15 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/.

Figure 9. Planned IUC System



Design

The Tunisian IUC will be a **back-end record locator stored only in the RIUC database** and will not be seeded in or stored in other databases (for example, as done in India, Estonia, and other countries). Rather than incorporating the IUC into sectoral systems, sectoral identifiers will be mapped to the IUC within the RIUC database. This is a deliberate design—enshrined in the IUC's draft enabling legislation—to protect privacy by limiting the proliferation (and potential misuse) of the unique number.

Under this architecture, it appears that the RIUC will facilitate identity verification and communication across sectoral systems by acting as a central translator. For example, if the social sector needs to verify a child's school enrollment, it could send a request to the RIUC along with the social identifier, and the RIUC would map this to the student identifier in order to facilitate the query. With this functionality, the IUC system has the potential to help rationalize and simplify the management of various identity registers, reduce instances of identity fraud, and simplify administrative procedures for citizens, while limiting the distribution of the IUC itself.

Although the system has not yet been fully implemented, a number of key decisions have already been made with regard to governance, coverage, the development of the RIUC database, deduplication procedures, the IUC number format, and the services it will provide for different sectors. Some of these choices have been specified in the new draft law on data protection that will support the IUC, while others have been taken by the project managers.

Enabling Legislation

The technical characteristics as well as the governance of the IUC system will be largely defined by a new organic law, the Personal Data Protection Law (LPDP), which was submitted to the National Assembly in March 2018 and has been debated in parliament since June 2019.[16] The LPDP—discussed further in section 4—will update Tunisia's current general data protection law to reflect the right to privacy in the new

16 Discussion at the committee on rights, freedom and foreign relations: http://arp.tn/site/projet/AR/fiche_proj.jsp?cp=101988.

constitution, clarify gray areas, and harmonize Tunisian law with new European data standards, including Convention 108+ (to which Tunisia acceded in 2017) and the General Data Protection Regulation (GDPR).[17] In addition, it includes specific enabling legislation for the IUC, which is summarized in Box 3. As specified in Article 75, more detailed specifications for the system will be issued by governmental decree.

Box 3. ID-Related Articles in the Draft Data Protection Law

In its current draft, there are a number of articles directed related to the IUC (translations by the authors, which are not validated), including the following:

Article 75: The "Register of the unique citizen's identifier" will be created, including its objectives and the personal data that it will contain, via a governmental decree. It will be maintained and managed by the MALE.

Article 76: The holding and management of the IUC register are subject to the same conditions and arrangement applied to the management of personal data, and the persons authorized to utilize the IUC are obliged to facilitate audits led by the INPDP, and as such are obliged to appoint a data protection officer.

Article 77: The IUC shall be attributed to (i) every person registered at birth in the REC [civil register] (ii) any person of Tunisian nationality born in a foreign country and registered at the Tunisian diplomatic or consular mission of that country (iii) any person having acquired Tunisian nationality. The data associated with these persons must be kept for 30 years after the death or after the loss of nationality.

Article 78: It is forbidden to assign the same IUC to more than one person and to assign more than one IUC to a person. The IUC code should not contain identifying information. Its objectives, its content, its technical characteristics, and the rules for maintaining and managing its register will be defined by a government decree after the opinion of the INPDP.

Article 79: It falls to the MALE to set up an online system allowing all citizens to be aware of all operations related to their IUC and the institutions that have used it.

Article 80: Use of the IUC is forbidden except by public or private agents in charge of managing a public establishment whose justification for using the IUC has been issued on a governmental decree after the opinion of the INPDP.

Article 81: It is forbidden to print the IUC on official documents issued by Tunisian state services except administrative correspondence between the public or private structures mentioned in the previous article.

Governance and Oversight

MALE is the overall project lead (*maître d'ouvrage*) for developing the RIUC in close partnership with MTCEN, which provides technical direction of the project management office (PMO), and the CNI, which is responsible for implementing the database and information systems. Strategic management (pilotage strategique) for the project is provided by the steering committee (COPIL), which is also led by MALE and includes members from a variety of stakeholders, including MTCEN, CNI, INPDP, Ministry of Interior, Ministry of Public Administration, National Institute of Statistics (INS), Ministry of Finance, MAS, and more. An operational committee (COOP) led by MTCEN meets monthly to oversee and validate technical decisions, and consists of representatives from MALE, INPDP, INS, CNI, MAS, Ministry of Health, Ministry of Education,

17 Article 24 of the 2014 Constitution states that, "The state protects the right to privacy and the inviolability of the home, and the confidentiality of correspondence."

and the Ministry of Interior. In addition, a technical task-force—consisting of MALE, MTCEN, and CNI—meets weekly, and other ad hoc work groups are convened as needed to address specific technical issues.

The existing governance structure is intended for the startup phase only. Eventually, an IUC "Management Body" (*Organe de Gestion de l'IUC*, or OGI) will be created to operate the IUC. Although the organizational and operational parameters for the OGI have yet to be defined, the current plan is for it to be housed within the Directorate General of Informatics within MALE. The INPDP will continue to serve in an oversight role for the IUC, including approving users of the IUC system and conducting audits (Articles 76 and 80 of the LPDP, see box 3).

Coverage

According to Article 77 of the LPDP, the IUC will be attributed at birth and cover all Tunisians resident in Tunisia, naturalized citizens, and Tunisian citizens living abroad. Because the RIUC will pull from both CIN and CR records, it should cover a large majority of the existing population given the high coverage of these combined systems. However, it is unclear whether there will be an effort to enroll the small proportion of Tunisians who were never registered at birth and do not have a CIN,[18] and if so, what this process would look like.[19] Furthermore, there are currently no immediate plans to include foreign residents or other nonnationals in the system in order to make the RIUC a true "population register." [20] However, the Border Police (Police aux frontières) operate a database of residents in Tunisia that could be integrated in the future. Furthermore, the IUC number has been structured such that the left-most digit (a "0" for initial citizen enrollments) could be used to signify nonnationals in the future.

Citizens will remain in the RIUC database with a unique number for their lifetimes, and for 30 years after their death or the loss of Tunisian nationality, at which point their data will be anonymized or deleted (LPDP Article 77); however, a record of the IUCs assigned to the deceased will be maintained indefinitely to ensure that they are not reassigned.

RIUC Database

The CNI has piloted the initialization of the RIUC database by cleaning and deduplicating copies of core attributes from the CIN and *Madania* databases (see Table 12), and then reconciling the two. As of February 2018, the database contained about 14 million records, including living citizens and those who died within the past 30 years. When the project is fully implemented, it will establish permanent links with both systems so that the RIUC remains updated with (1) new births, (2) deaths, (3) new family structures (including marriages, divorces, and children), (4) changes or edits in CR information, and (5) new CIN numbers. In addition, the RIUC will be linked to a Ministry of Justice database in order to sync attributes related to legal status and will include a mapping of IUC numbers to sectoral identifiers (process also to be defined) to facilitate intersectoral identity queries. Eventually, people will be able to self-declare their address in the system, but this process has yet to be defined.

---

18 While the precise number of people who are not registered in the countries foundational ID systems is not known, extrapolating from the UNICEF-declared birth registration rate of 99 percent would translate to about 115,000 children under the age of five who were not registered at birth. Similarly, if we assume 90 percent coverage of the CIN (likely a conservative estimate, see earlier section), this could mean that about 830, 000 Tunisian adults do not have the card. Although these numbers may be relatively small, it is often the most marginalized and vulnerable sections of the population who lack ID (for example, poor rural women, and so on) and who may be excluded from access to programs that require an ID.

19 Citizens who do not appear in the Madania database but have a CIN will not be included in the initialization of the RIUC system. However, they will be identified in an "anomaly file" and included later after an adjudication process. However, there appears to be no concrete plans for how to include those nationals who are in neither *Madania* nor the CIN database (see previous footnote).

20 Initially, the draft LPDP did not refer only to citizens, but to those in the civil register. However, the text has since been modified to refer only to citizens. In the plans for the initialization of the RIUC database, noncitizens who have records in the Madania system (that is, their births, deaths, or marriages were registered) will be initially excluded, pending further plans for incorporating nonnationals.

Table 12. Data to be Stored in the RIUC (in both Arabic and French)

Category	Attribute	Source
Biographic	**Last name***+ **First name***+ **Father's first name***+ **Paternal grandfather's first name***+ **Mother's last name***+ **Mother's first name***+ **Sex***+ **Birth date***+ Birth location+ Marital Status and IUC of current spouse IUCs of parents, children (family clusters) Date of death Place of death	*Database creation:* CR (*Madania*)/CIN database to be joined and reconciled *New enrollees and updates:* Pushed from CR (*Madania*)
	Declared Address	Self-declared and validated through a process to be defined by OGI
Identity numbers	IUC number	Generated after deduplication and reconciliation of CR and CIN data
	Birth certificate reference number+ Birth certificate reference number year+	CR (*Madania*)
	CIN number	CIN database
	Sectoral identifiers (e.g., IS, tax ID (*matricule fiscale*), etc.)	Sectoral databases (process to be defined)
Legal	Acts and decisions relating to legal capacity	Ministry of Justice
Note: * **Eight attributes used for deduplication** +Attributes reconciled against CIN.		

Deduplication

Given the relatively small size of the Tunisian population (less than 12 million) and concerns over privacy, implementers have chosen demographic rather than biometric deduplication. A deduplication algorithm relies on eight primary attributes: last name, first name, father's first name, grandfather's first name, mother's first name, mother's last name, birth date, and sex.[21] Through this process, the IUC system will ensure statistically **unique identification** of the population (Article 78 of the LPDP) in the sense that:

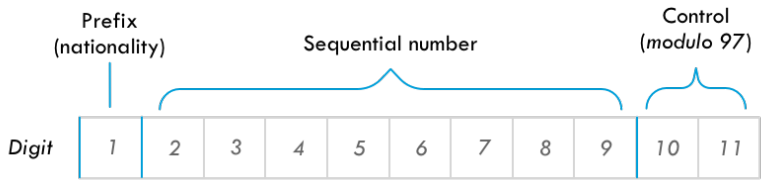
- All citizens registered in *Madania* will have an IUC, except those deceased 30 years before the initialization of the database
- No citizen can have more than one IUC, even if they have two birth certificates
- Each IUC is assigned to only one citizen, for their lifetime and 30 years after death

21 These criteria were used for deduplicating the Madania database prior to reconciliation with the CIN database; additional measures were also taken to deduplicate the CIN data before reconciliation (for example, removing people with multiple CIN numbers).

IUC Number

The IUC will be an 11-digit number, consisting of a single-digit prefix, an 8-digit sequential (nonrandom) root, and two control numbers, as shown in figure 10. Initially, the prefix was intended to signify whether the person had a CIN. Under the current design, however, it will be set to 0 for all Tunisian nationals. Should the system be expanded in the future to incorporate nonnationals, the idea would be to structure their IUC numbers beginning with a 1.

Figure 10. Planned Structure of IUC Number



As described above, **the IUC number is intended to remain private**. According to Article 81 of the LPDP, it cannot be visible on any official documents, such as birth certificates or ID cards. As a result, it *will not be known to people or used directly for authentication* (for example, like India's Aadhaar). Instead, it is the unique key stored in the RIUC system, which will primarily be a platform for back-end identity verification.

Services

Users—including government various agencies and ministries, as well as people themselves—will access the RIUC system through two mechanisms:

- **Access platform for public and private agencies:** Public and private entities involved in the provision of *public* services will be able to access certain data through a platform based on partnership agreements with the OGI (Article 80 of the LPDP). This platform will be linked to the national interoperability platform (TunXRoad) and designed to meet a number of requirements, including secure transactions with controlled access, audit trails, and technology neutrality that requires minimal adaptation by users.
- **Citizen access portal:** People will be able to view their personal data and how it is being used through an online portal (Article 79 of the LPDP). This portal will perform a number of functions, including allowing citizens to update certain attributes, see the history of consultations, and clarify how it has been used.

Initially, the primary services facilitated through the IUC platform include verification of life, sharing basic identity attributes to prepopulate forms, and verifying basic attributes and identifiers, as shown in table 13. As described above, the eventual goal is also for the RIUC to serve as a dictionary that allows different functional systems to exchange information via their own, separate identifiers.

Table 13. List of Early Services Developed for the RIUC

Service	Description	Initial Relying Parties
Verification of life/ death	This service makes it possible to query whether or not a person has died (based on death registration and certificates from Madania). The goal is to eliminate the need for citizens to provide civil status records as proof of life and optimize benefits management. **Input data:** • Place of birth, date of birth, sex, first name, last name, father's first name, mother's first name, mother's last name, grandfather's first name • OR Social identifier (IS) • OR reference number of the birth certificate **Output data:** Response indicating if the person is alive or deceased, and–if deceased– date of death and death certification.	MAS, CNSS, CNRPS, CNAM
Verification of biographic attributes	This service makes it possible to query information from a person's birth records. It can be used to: (1) prepopulate basic ID attributes (reducing the risk of data entry error); (2) check that data in the querying databases matches the person; and/or (3) to complete missing information in the querying database. The goal is to eliminate the need for citizens to provide birth extracts. **Input data:** • Place of birth, date of birth, sex, first name, last name, father's first name, mother's first name, mother's last name, grandfather's first name • OR Social identifier (IS) • OR reference number of the birth certificate **Output data:** First name, last name, date of birth, sex, father's name chain, mother's name chain.	Ministry of Education: student registration MAS, CNSS, CNRPS, CNAM: enrollment
Verification of family status	This service will permit queries about the affiliate's marital status. The goal is to eliminate the need for citizens to provide civil status records and optimize benefits management. **Input data:** • Place of birth, date of birth, sex, first name, last name, father's first name, mother's first name, mother's last name, grandfather's first name • OR Social identifier (IS) • OR reference number of the birth certificate **Output data:** Whether married or unmarried, and if married, the date of marriage.	MAS, CNSS, CNRPS, CNAM

Verification of spouse information	This service will permit queries about the affiliate's spouse. The goal is to eliminate the need for citizens to provide civil status records. **Input data:** • Place of birth, date of birth, sex, first name, last name, father's first name, mother's first name, mother's last name, grandfather's first name • OR Social identifier (IS) • OR reference number of the birth certificate **Output data:** First and last name of spouse.	MAS, CNSS, CNRPS, CNAM (via OracleForms, Java)
Source: MALE and MTCEN.		

Timeline

The IUC project was launched in 2017. As of 2019, major project milestones and future plans to make the IUC fully operational include:

- 2019:
  - A first version of the IUC information system (with an RIUC of nearly 15 million records) went into production in September 2019 allowing access to the RIUC data (via the queries described in Table 13) to the MAS, CNSS, CNRPS, CNAM, and education information systems.
  - Launch of the procurement process for the development and deployment of a more elaborate version of the IUC information system.
  - Launch of the procurement process for the redesign of the civil registration system (Madania), the main source of the RIUC data.
- 2020: Implementation and deployment of new IUC and *Madania* systems.
- 2021: Full-scale implementation of the IUC and *Madania* systems.

In parallel, there are ongoing efforts to increase the accuracy of the initialized RIUC database and to identify duplicates and errors in the source data (*Madania* and the CNI database). After this reconciliation is complete—planned for 2020 or early 2021—there will be a campaign with local registrars to improve the reliability of their data, anticipated for 2020-2024, in parallel with the redesign of the Madania system.

3. Functional ID Systems

In addition to the foundational systems described above, the GoT also operates a number of functional ID systems for sectoral use. These systems play a critical role in identifying the population eligible for a particular service, right, or administrative procedure—for example, cash transfer beneficiaries, taxpayers, voters, and so on—and in some cases issuing their own credentials for authentication. Tunisia's most well-developed functional ID systems with the widest coverage are those used to manage the country's social protection programs. As such, this section provides an in-depth look into various social protection systems, along with shorter overviews of identification in other sectors, including health, education, and taxes.

Social Protection

Sector Overview

Tunisia's social protection system consists of noncontributory programs (that is social assistance/social safety net programs) and contributory programs (that is, social security including pension and health insurance):

- There are two main noncontributory social assistance programs, notably a cash transfer program called the National Assistance Program for Families in Need (P*rogramme National d'Aide aux Familles Nécessiteuses*, or PNAFN) and an indigent health insurance program called AMG1/2.[22] These programs are administered by the Ministry of Social Affairs (MAS) and currently cover about 30 percent of the population.
- For the contributory system, there are two social security funds, one for the private sector (*Caisse nationale de sécurité sociale*, or CNSS) and the other for the public sector (*Caisse nationale de retraite et de prévoyance sociale*, or CNRPS). These social security funds are responsible for collecting contributions and processing payments for pensions, benefits to widows and orphans of pensioners, death benefits, and social loans. While coverage of pension systems is high, about 50 percent of the current labor force contribute to one of the two main social security systems.[23]

Consequently, all individuals enrolled in the CNSS and the CNRPS are automatically eligible for national health insurance program, administered by the national health insurance fund (*Caisse nationale d'assurance maladie*, CNAM).[24] Combined with social assistance program beneficiaries of the health indigent program, it is estimated that about 90 percent of the population are covered by health insurance programs in Tunisia.

There has been a concerted effort among the MAS, the CNSS, the CNRPS, and the Center for Research and Social Studies (CRES) to modernize the delivery system of these social protection programs, including the improvement of beneficiary registers and identification. The main activities include:

---

22 The PNAFN is targeted at the poorest of the population, covering about 8 percent of the population. In addition to a cash transfer, PNAFN beneficiaries also have free access to free healthcare in public institutions (that is, AMG1, *Assurance Médicale Gratuite de type 1*). An additional 22 percent of the vulnerable population who are unable to be a part of contributory health insurance system receive a subsidized health card (AMG2 or *Programme de carnet de soin à tarif réduits*), allowing them to access medical care in public health facilities by paying a fixed annual fee.

23 World Bank. 2019. *Tunisia Public Expenditure Review*. Washington, DC: World Bank.

24 The CNAM was established in 2007 with the goal of unifying various insurance and health benefits schemes and increasing the coverage of health services by private providers. It provides health insurance plans, compensation schemes for work-related accidents (*Accidents de Travail et Maladie Professionnelle* or ATMP), sickness benefits provided by social security schemes, and other assistance.

- Developing and improving the **information management systems** of the MAS and social security funds, including the implementation of a **social identifier (IS)** and **interoperability platform** for identity management and data exchange between noncontributory and contributory schemes.
- Developing an updated **beneficiary database** of the main social protection programs (PNAFN and AMG2) which could provide the foundation for a future of **unified social registry**, and the development of a targeting tool.
- Issuing a **new card** (led by CNAM) to improve the authentication of beneficiaries at hospitals, replacing current paper-based cards.

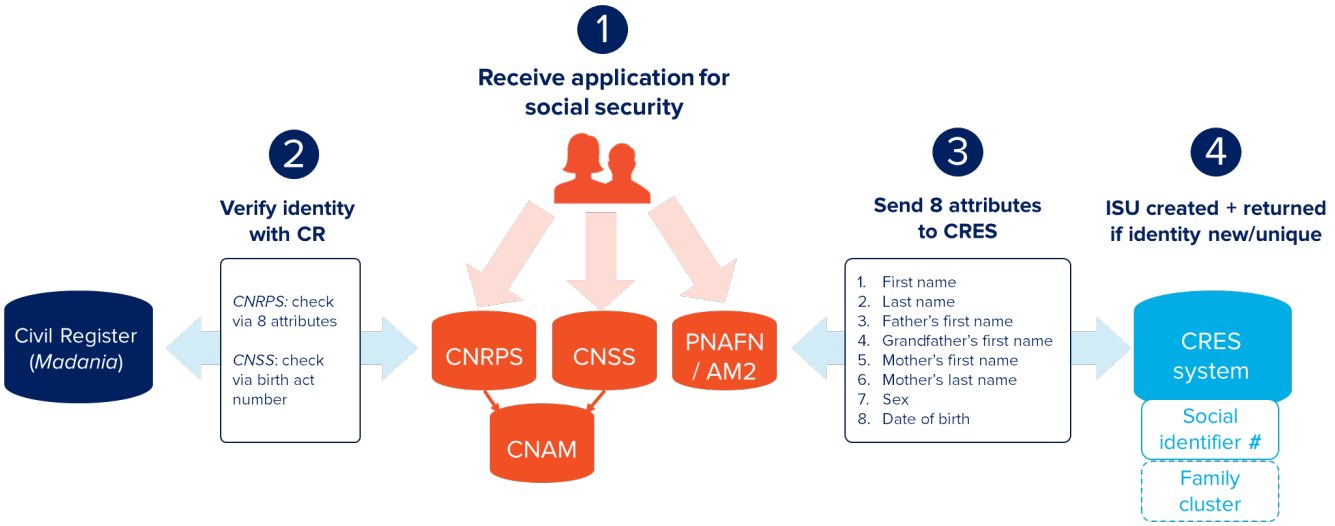
The following section discusses two of these projects in detail: the social identifier (IS) and CNAM card.

Social Identifier (IS)

The initial and main objective of the IS is to identify individuals across contributory and noncontributory systems to improve the targeting of social assistance programs. Specifically, with the IS, the MAS can verify the social security contribution of social safety net beneficiaries more efficiently. The IS project began in 2003 as a collaboration between the two social security funds (CNSS and CNRPS), and was later extended to incorporate the CNAM, as well as the noncontributory social protection programs run by MAS. The IS system is operated by CRES, which issues unique numbers[25] for each beneficiary across the social programs, based on the data provided by the MAS, the CNSS, and the CNRPS.

The IS has currently been assigned to over 10 million individuals (as of May 2019), with the CNSS as the major feeder for the database (about 80 percent of the data come from the CNSS). This number includes those who are no longer active and potential duplication in registration. To improve the process and the data, an audit of the IS was carried out in 2019, and the recommendations are expected to be implemented.

Figure 11. Generation of the IS



25 Eventually, CRES also plans to include family clusters—that is, links between the identities of family members—which are necessary for household-based targeting for social protection programs. It is unclear whether this could/will leverage similar plans for the Madania system.

As shown in Figure 11, the CNSS, CNRPS, and the MAS send their data to CRES, including the eight criteria detailed in Figure 11—which, notably, are the same criteria used to deduplicate citizens in the RIUC. CRES uses this information to deduplicate beneficiaries and determine whether or not they have already been assigned an IS (for example, as happens when a person changes their employment sector). CRES then generates the IS number (or finds an existing number) and return this to the fund database. The CRES application contains a control algorithm that refers to a dictionary of names in Arabic to avoid transcription problems.

Table 14. Summary of the IS

Coverage	Social assistant program beneficiaries and their family members Contributors to the social security systems and their dependents
Number of individuals with the IS (actual)	10.8 million as of May 2019 (87% of the country's population) • About 8.1 million from CNSS (79% of the database) • About 1.7 million from CNRPS (14% of the database) • +1 million from MAS (7% of the database) [It is expected that this number will reach 2 million when MAS completes updating the information of all PNAFN and AMG1/2 beneficiaries]
Biographic attributes	Eight criteria are required to deduplicate a person's identity and generate the IS: 1. First name 2. Last name 3. Father's first name 4. Grandfather's first name 5. Mother's first name 6. Mother's last name 7. Birth date 8. Sex In addition, the following information is collected where available: (9) address, (10), civil status (single, married, etc.), (11) CIN number, (12) birth certificate number, (13) place of birth, (14) nationality.
Biometric attributes	None
Deduplication	Via the 8 attributes above (demographic only)
Credential type	Identifying number only, no card or other credential issued
Number format	10 digits: 8 sequential numbers (anonymous) plus 2 control digits
Database architecture	Centralized database
Databases with which system exchanges information	CNRPS (daily) CNSS (daily) MAS (once every three months)
Database technology	Oracle 12c, 8GB
Backup and disaster recovery	Daily full backup with Backup Exex 2014, no emergency site

Since it began implementation, the integration between the IS and social programs has made significant progress under the cooperation between MAS, CRES, CNSS, CNRPS, and CNAM. Table 15 summarizes these advances along with basic information about these programs.

Table 15. Summary of IS Integration for Main Social Protection Systems

	MAS	CNSS	CNRPS	CNAM
Who is covered	Safety assistance program beneficiaries (PNAFN and AMG1/2)	Private sector employees and their dependents	Public sector employees and their dependents	Employees insured by CNRPS and CNSS and their dependents
Target coverage	2.3 million	About 9.6 million	About 1.8 million	About 8.5 million
IS coverage	1 million (53%)[a]	8.1 million (84%)	1.7 million (95%)	5.8 million (83.5%)[b]
Biographic data	Planned: in accordance with the new CNAM cards	**Identifying data (8 attributes):** first name, last name, father's first name, grandfather's first name, mother's first name, mother's last name, birth date, and sex **Program information:** e.g., regime, location of birth, dependents, salary **Additional identifiers:** birth certificate number, CIN number and date of issue	**Identifying data (8 attributes):** first name, last name, father's first name, grandfather's first name, mother's first name, mother's last name, birth date, and sex **Program information:** e.g., dependents, etc.	Planned: in accordance with the new CNAM cards
Biometrics	None	None	None	None
Deduplication	Via the IS	Demographic deduplication before CNSS number generated	Via the IS	Via the IS
Credential	Planned: extension of CNAM card to cover MAS beneficiaries	Only CNSS number issued specific to regional office where enrolled, 10 digits: 1 activity code 7 digit root 1 account code 1 control digit	Only CNRPS number issued	*Planned:* CNAM card (2D barcode)
IS integration	Newly registered people are sent to CRES, as they are registered in MAS's new database (frequency not determined)	Every day, new CNSS enrollees and updates are sent to CRES via FTP server.	New applicants are verified against CRES database to recover/ assign an IS. Data is sent via FTP server request to CRES several times a day.	The CNAM uses the IS as mandatory data to register for health insurance; beneficiaries without the IS are systematically redirected to the affiliate fund for IS attribution or data correction.

Integration with other databases	CNSS CNRPS Madania	**CNAM:** CNSS sends data to CNAM every 2 weeks to update IS records and errors (via Oracle database), and twice a week (via FTP server) with new enrollments. **Madania:** CNSS sends batch requests to verify birth information via the birth certificate number.	**CNAM:** CNRPS sends data to CNAM, including monthly data dumps with pension information, and daily updates (via FTP server) on newly insured people. **Madania:** CNRPS sends on-demand requests to verify birth information via the 8 attributes.	**Ministry of Health:** bills **Banks/Post**: data on transfers **Ministry of Finance:** data on care providers **Madania** (process uncertain)

Source: TALYS Consulting. 2019. IS Audit Report.

Note: a. Among social assistance program beneficiaries, about 30% of members are found in the social security database when crosschecking with the IS; b. Currently, there are children and spouses who are in the CNAM database but not in the social security databases and they are trying to address this issue as the entitlement of health insurance stems from the social security contribution.

The sections below describe the integration of the IS into the separate social protection databases, along with persistent challenges.

MAS Database for Social Assistance Programs (Noncontributory System)

Integration of the IS into the MAS database began in 2016 with the drive to develop the beneficiary registry of social assistance programs, notably the PNAFN and AMG1/2. Thus far, out of a total of about 2.3 million beneficiaries (belonging to 0.9 million households), some 1.3 million individuals have had their data entered into MAS's new information management. However, the IS has been assigned to about 1 million people. This discrepancy has two causes: first, there is a delay/irregularity in sending the data from the MAS to the CRES in order to assign the IS; second, of the records received by the CRES, 20 percent were rejected because of a lack in key information needed for the IS generation. The IS coverage is expected to increase as the MAS collects and sends more data to the CRES and the rejected cases are corrected.

As a result of the IS assignment, about 30 percent of social assistance program beneficiary family members were found in the social security database (that is, CNSS and CNRPS database). This means that the IS will greatly facilitate MAS's ability to verify the administrative data related to the wellbeing of potential and current beneficiaries. Specifically, the MAS will have a greater capacity in (re)assessing the need and the eligibility of social protection program beneficiaries based on the social security contribution status of all family members. Currently, social workers are manually crosschecking the CNSS database to verify the social security contribution of individual members of beneficiary households. It is expected that this process will become faster and more efficient through a new data exchange platform and new targeting mechanism[26] that would incorporate information related to the CNSS and CNRPS, which can be verified automatically using the IS for communication between databases.

26 In addition, a new targeting tool will provide additional information on the wellbeing of households using objective criteria and a transparent procedure. A proxy means test (PMT) is currently being developed based on the official INS survey, while a hybrid means test for the administrative data related to the income is also being explored as a next step.

Social Security Funds (Contributory Systems, CNSS and CNRPS)

Private-sector employees enroll in the CNSS at one of the 49 regional and local offices by providing their birth certificate, birth certificates for their dependents, and their CIN, among other documents. As with the CNRPS, eight attributes are then collected: first name, last name, father's first name, grandfather's first name, mother's first name, mother's last name, birth date, and sex. The applicant's identity is then verified, and a search in the CNSS database is performed to determine if a person with the same sex, name, and birth date has already enrolled. If the applicant is not found in the database, then the applicant's attributes are recorded and a CNSS number is issued from the bank of numbers reserved at the office. Because the number changes when people change regimes, it does not remain unique for the beneficiary over time, and the probability of two people having the same CNSS number is about one in forty thousand. The CNSS systematically sends the IS creation request for the new registrations, changes in regime or situation, as well as corrections to the identity of attributes of beneficiaries.

To enroll in the CNRPS, public-sector workers — through their employer (a ministry or public company) — must provide substantiating documents including their birth certificate (in Arabic), CIN, and certification of employment at one of 24 regional registration centers and/or seven local centers. The identity of the applicant is verified using eight attributes (in Arabic): first name, last name, father's first name, grandfather's first name, mother's first name, mother's last name, birth date, and sex. This data is first sent to the central CNRPS database, which then sends the eight attributes for certification to CRES. CRES then either (a) returns the persons' IS number if one has already been created, or (b) issues a new IS number, which is then recorded in the CNRPS database. The CNRPS also verifies birth registration information by sending digital queries to the CR's Madania system using the same eight criteria. Management rules impose a 48-hour processing window for when the IS should be attributed after the request is sent from the employer.

Despite the progress made, there are some lingering issues with the integration of the IS into the CNSS and CNRPS systems:

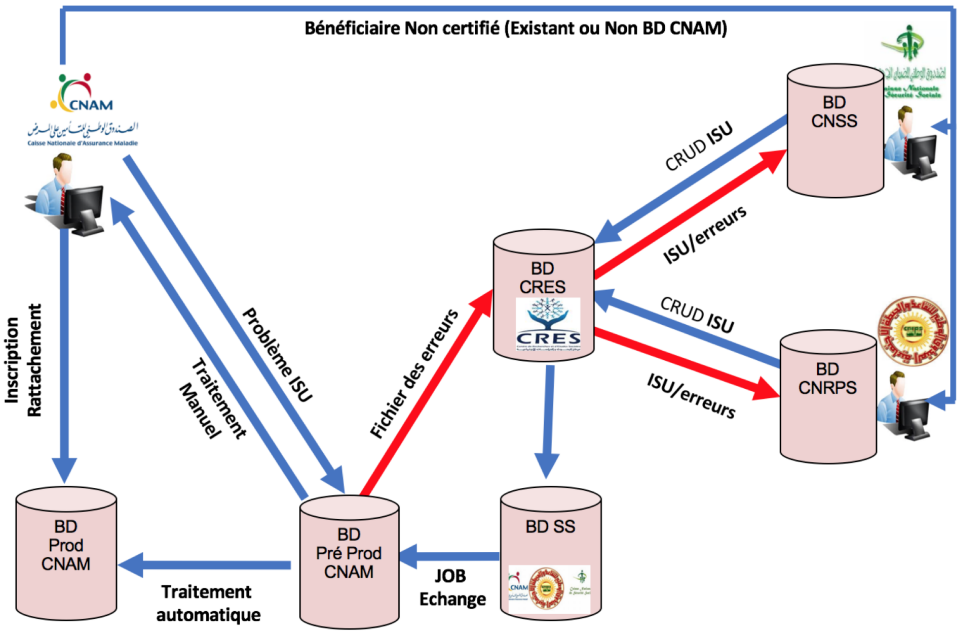
- Lack of the eight attributes needed to issue the IS (about 2 percent for the CNRPS).
- A data gap between the social security funds (CNSS and CNRPS) and the CRES is possible (for example, the CNSS does not directly send updates to the CRES, and there are no management rules for the time to issue an IS to the CNSS data).
- Not all family members are always declared to the social security funds. This is primarily because of the current practice for CNAM enrollment that information on spouses, children, or dependents is often updated at the CNAM only, although their health insurance entitlement comes from the contribution to the CNSS/CNRPS. As a result, family member information is often not fully updated at the CNSS/CNRPS, and an IS is not issued to all family members (for example, only 30 percent of families had similar family cluster information in two databases of the CNAM and the CRES in 2018).[27]
- The CNSS's information system remains partitioned and composed of several independent applications which use the internal ID (CNSS number), not the IS.
- Data exchange between the CNSS and the CNAM is based on the CNSS number and not the IS.
- After the death of a pensioner, surviving family members receive their pension through the deceased's IS number (plus a prefix), and so they are not themselves identified with an IS in the pension management information system (the IS is granted through the registration in social insurance so that they can benefit from health insurance).

27 Talys Consulting. 2019. IS Audit Report.

Health Insurance Fund (CNAM)

Previously, the CNAM database was populated based on the CNRPS and CNSS, which send periodic records of their beneficiaries who are automatically covered by CNAM. As such, new enrollees in CNAM should have the ISs (or CNSS numbers) they received when registering with one of the two social security funds. However, given the urgency of extending health insurance benefits, there was a period where CNAM proceeded to enroll and provide benefits for family members (spouses and children) who were not registered with CNSS or CNRPS and did not yet have an IS. In order to address this issue, enrollment was halted in 2014 and again in 2016, after recommendations to organize a media campaign to ensure that all family members have an IS first. This involves directing them to first register with the CNRPS or CNSS for an IS to be issued, before enrolling in CNAM (see Figure 12).

Figure 12. CNAM Beneficiary Verification Process



Source: CNAM presentation on IS.

At present, however, the IS is not currently being used by CNAM. Specific issues with integration include:

- Data for CNAM are collected and entered in French (rather than Arabic) and do not include all eight attributes needed for verification.
- There are data entry errors (for example, date of birth, last name, CIN numbers).

Plans for Health/Social Protection Cards and Authentication (CNAM Cards)

Currently, patients access health insurance benefits through a paper-based ID card, and the claims process between beneficiaries, healthcare providers, and CNAM is largely manual. In mid-2018, CNAM launched a project with the objective to modernize the administration of the fund, reduce overall costs, allow a direct data transfer between healthcare providers and CNAM, and improve the quality of services to citizens. The project consists of three components, including: (1) implementing an Electronic Data Interchange System (SEED) between the fund and healthcare providers, (2) improving identity access and security management, and (3) issuing a new card to replace the current paper-based cards. [28]

Despite earlier plans for a smartcard, CNAM has decided to implement a basic card with a 2D barcode to store encrypted data, including the IS number, that will allow for authentication through the CNAM platform. This card will strengthen the governance of health insurance through an improved authentication of people in accessing health services. Because health insurance is administered at the household level, only one card will initially be issued per family, while a future plan includes issuing additional cards to other eligible household members. The distribution of these new cards for beneficiaries of CNAM—the regular, contributory health insurance program—began in April 2019.

In addition, using the same solution/technology, MAS has also started distributing the cards to beneficiaries of the indigent health insurance program so that in the future the same card could be used to avoid distinguishing between contributory and noncontributory beneficiaries. By using the same credential across programs, the new health/social protection cards will enable the administration to better manage people changing their status between indigent and regular programs (that is noncontributory and contributory systems) [29] through a back-end system rather than indicating their status visibly on the cards. This also helps to protect privacy and reduce the potential social stigma experienced by beneficiaries of indigent programs. Once cards are issued to the target population of beneficiaries, about 90 percent of Tunisia's population will have a more convenient and secure way to authenticate themselves when they access health services.

Ways Forward

Based on the findings from the IS audit, CRES has prepared a roadmap to continue improving the IS.[30] For example, the action plan includes: (i) synchronization of the IS with different data, particularly the *Madania*, through a web service; improvement in dictionary management (for example, defining the access, specifying the workflow, harmonization of dictionary (for example, first and last name); (ii) implementation of a new platform to follow up on issues related to the data quality (this will entail defining the data exchange protocol, users, rules for data control); (iii) specifying the modalities to enhance data reliability (for example, automatically crosschecking identities with *Madania* for stock and new/flow data, detecting duplicates); and (iv) redesigning the process to assign and modify the IS for different stakeholders, including organizational and governance structure.

28 MAS had been planning to roll out a more advanced card for health insurance beneficiaries for nearly a decade. However, three earlier rounds of procurement were unsuccessful: http://www.realites.com.tn/2017/09/la-cnam-lance-la-smart-card-au-profit-de-ses-affilies/.

29 In the long term, these basic cards may be replaced by more sophisticated solutions when they become available under national authentication/e-ID card projects.

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

Health Sector

Public hospitals at levels 2 and 3 (that is, regional hospitals and university hospital centers) currently each have their own independent information system for identifying patients locally. These hospital-level ID numbers are ten digits and include the year the person was registered and a six-digit sequential number by facility that restarts at zero each year. In addition to the patient's name, sex, birth date, governorate of birth, marital status, and mother's and father's first names, hospital information systems also record a person's CIN number and CNAM card number. However, this information is not captured systematically and there is a risk of assigning a different ID for the same patient on different medical visits.

Although these identifiers create a record for patients at a given facility, there is no centralization or interoperability of these systems, meaning that a person must register anew at each facility, and will be entered in multiple facilities with multiple numbers. In addition, there is no interoperability between public and private health providers, which is an issue as many patients use multiple facilities of both the public and private kind. As a result, patients do not have complete, portable, electronic health records, and hospitals do not have a unified view of patient history.

Currently, the Ministry of Health (MOH) is conducting a planning study for improvements to the hospital information and patient identification systems. While there is already an agreement that this system will incorporate the IS, there is also the potential that this system could leverage the IUC in the future—for example, to cover the small percent of the population that will not have an IS. [31] Furthermore, given the high rate of institutional births in Tunisia, there is the potential for further cooperation between the MOH, the civil register, and the IUC in order to integrate the unique identifier into the birth registration process. Lastly, integration between the health system CNAM could also improve access to the health services and the monitoring and management of health insurance.

Education

The Ministry of Education has information systems that manage data on students in primary and secondary school at public institutions. Previously, students were issued with institution-based numbers that were not centralized or interoperable, meaning that a student would receive a new number each time they moved schools with no link to maintain continuity in student records. Beginning in 2018, the Ministry of Education worked with MTCEN and MALE to simplify the enrollment process for secondary school students using the *Madania* system. In 2019, parents preregistered their children for primary school online, and no longer need to bring birth certificates, leveraging the e-madhmoun system described previously. This has been scaled up to cover secondary school enrollment and will cover private schools as well during a later phase. In the new system, students are identified by a unique number that is generated after verifying the student's existence in the civil register and mapped with the IUC. As of 2019, this system covered about two million students. In order to maintain this system, the Ministry of Education must ensure that any new registration goes through this process especially during the school years.

Taxes

Within the Ministry of Finance, the General Tax Directorate (Direction générale des impôts) maintains a database of taxpayers and issues a tax ID (matricule fiscal). As of 2015, about three million people were registered in the system, and of these, about 566,000 are identified by their tax IDs and are active taxpayers. In order to enroll in the system, taxpayers must provide their CIN number, along with their name, birth date, address, and occupation. The Directorate also receives information from employers (and the CNSS via the INS), the Ministry of Interior (regarding traffic violations), and the Ministry of Labor (on other infractions).

31 About 90 percent of the Tunisian population is expected to be covered by either contributory or noncontributory health insurance schemes, and will therefore have been issued an IS.

4. Legal Framework

Tunisia has a relatively comprehensive legal framework for its ID systems, including organic laws and decrees that empower identification and civil registration agencies, govern the processing—that is, collection, storage, use, transfer, and so on—of personal data, include regulations for data protection, and establish an independent agency to oversee data processing in accordance with this law (the INPDP). This legal framework was enumerated in the 2015 report commissioned by the MTCEN, and therefore a detailed cataloging of Tunisia's laws related to identity was not the focus of this report. However, this section provides a brief overview of the draft LPDP and draft digital code (Code numérique), both of which are in different stages of consideration by the Tunisian National Assembly. Each of these laws are critical to the implementation and management of the IUC, IS and other sectoral identifiers, as well as digital identity and trust services more broadly.[32]

Draft Organic Law on the Protection of Personal Data

As described above, the Tunisian National Assembly is currently considering a draft law on data protection (the LPDP) that outlines some basic design elements of the IUC (see box 3). In addition, this law will apply more broadly to all entities—public and private—that process personal data within the Tunisian territory, including the foundational and functional databases described above (LPDP Article 2). It is designed to update the existing 2004 law on data protection in order to clarify certain ambiguous areas[33] and harmonize it with the new 2014 constitution and with international principles on privacy and data protection, such as the GDPR and Convention 108+ of the Council of Europe, to which Tunisia acceded in 2017.[34] The draft LPDP was approved by the ministerial council in March 2018, and has been under the discussion at the National Assembly since 2018.

In particular, the draft law specifies the following rights, principles, and regulations for data processing, among others:[35]

- **Right to privacy and data protection:** The right to data protection (Article 1) which complements the right to privacy enshrined in Article 24 of the 2014 Tunisian constitution.
- **Oversight:** Data processing will be overseen by an independent public authority (Article 1) which will authorize the processing of personal data (Article 9). This authority is the INPDP, which was established by decree in 2007.[36]
- **Transparency.** Processing must be known to the public and approved by the INPDP, which will keep a register of authorized data processors on its website (Article 5). Data subjects also have the right to be informed about the existence of an automated decision-making process based on their data (Article 6).

---

32 ID4D has developed an additional tool to conduct a more in-depth analysis of the legal framework for ID, called the ID Enabling Environment Assessment (IDEEA). The current version of the IDEEA Guidelines can be found at https://id4d.worldbank.org/legal-assessment.

33 The law will replace or supplement the existing legal framework on this topic, including organic law 2004-63 on the protection of personal data: http://www.inpdp.nat.tn/textes.xhtml.

34 Seehttps://www.coe.int/en/web/data-protection/home/-/asset_publisher/RMbj8Pk1ApgJ/content/welcome-tunisia-new-party-to-convention-108.

35 Translations are by the authors and are not official. Consult the draft law in French and Arabic for the full, precise text. Article numbers in this section come from the 2017 version of the draft law in French; they may differ from those currently being discussed in the parliament, the text of which is in Arabic.

36 For the full text of Decree n° 2007-3003 in French and Arabic, see http://www.inpdp.nat.tn/ressources/decret_3003.pdf. The procedures for authorization for the processing of personal data by the INPDP can also be found in Decree n° 2007-3004 at http://www.inpdp.nat.tn/ressources/decret_3004.pdf.

- **Respect and do no harm:** Personal data must be processed fairly and transparency, and the principles that the processing of personal data must be carried out within the framework of respect for human dignity, privacy and public and individual freedoms and must not infringe a person's rights or do harm to their person or reputation (Article 8).
- **Minimization:** Data processing should be adequate, relevant, and not excessive in relation to the purposes for which data were collected (Article 8).
- **Storage limitation and the right to be forgotten:** Data may only be stored in a form permitting the identification of the persons concerned for a period not exceeding that required for the purposes for which they are processed (Article 8). Once the purpose of the data processing has been reached data controllers are require to destroy or anonymize data (Article 64).
- **Quality and accuracy:** The data controller must ensure that the data is accurate and up to date (Article 8). The data controller and the processor must correct, add to, modify, or update personal data and delete them if they become aware of their inaccuracy or insufficiency or if the purpose for which they have been collected is completed (Article 17).
- **Purpose specification:** The collection of personal data may only be carried out for lawful, determined, explicit, and declared purposes. The processing of personal data may be carried out for purposes other than those for which it was collected only if the data subject has given their consent or if the processing is necessary to safeguard a vital interest of the data subject (Article 9).
- **Sensitive data:** The processing of personal data which directly or indirectly reveals racial, ethnic or genetic origin; biometrics; location; religious convictions; political, philosophical, and syndicalist opinions and affiliations; health; or the sex life or sexual orientation of a natural person is forbidden unless carried out with the express consent of the data subject based on adequate information, or where such processing is necessary to safeguard the vital interests of the data subject in accordance with rules defined by this law. The processing of personal data related to infractions, their persecutions, penalties, preventative measures, or criminal records is not permitted except by the courts and paralegals within limits and under conditions fixed by the court. (Article 11).
- **Prohibition on linking a benefit to consent:** It is strictly forbidden to link the provision of a service or the granting of a benefit to a person to their acceptance of the processing of their personal data or the exploitation of their data for purposes other than those for which they were collected (Article 12).
- **Data security:** Any person who personally or through a subcontractor handles the processing of personal data must take all necessary precautions to ensure the security of such data and prevent third parties from modifying or consulting the data without the consent of the person concerned. (Article 13). Information regarding breaches of security must be reported to the INPDP within 48 hours and to the data subjects in a timely manner (Article 14).
- **Informed Consent:** The processing of personal data may only be carried out with the consent of the data subject who must be free, specific, informed, unambiguous, explicit and leave a written or electronic trail (Article 38). This consent can be withdrawn at any time (Article 39).
- **Right of access:** Allowing the person concerned access at reasonable intervals, without delay, to their personal data and the right to obtain a copy and to request corrections or deletion (Article 47).
- **Data transfers to other countries:** The transfer of personal data to another country is only allowed if that country provides an equivalent level of protection and requires the authorization of the INPDP. Transfer of data to other countries is prohibited when this is likely to jeopardize public security or the vital interests of Tunisia (Articles 35 and 36). Personal data processed by public corporations cannot be hosted outside the national territory (Article 132).

- **Exceptions to the law:** There are two exceptions to the law in accordance with Article 49 of the Constitution, including for purposes related to (1) national or public security, important financial or economic interests of the state, the impartiality and independence of the judiciary, and/or the prevention, investigation, or persecution of criminal offences, or (2) for the protection of the data subject or the fundamental rights and freedoms of others including the freedom of expression (Article 4).

In addition, the LPDP confirms the responsibilities of the INPDP—defined as an independent, financially autonomous, legally constituted body (Article 140)—including, but not limited to: authorizing data controllers and processes; receiving complaints and disputes under its jurisdiction; elaborating rules and guidelines for processing personal data; ensuring compliance with legal and regulatory standards; working with National Authority for Access to Information and other regulatory institutions to make decisions and guidelines on data access; and carrying out periodic assessments of compliance with data protection laws (Article 141).

Digital Code

The GoT has drafted a new Digital Code (Code numérique) designed to spur and regulate the development of a digital economy, which is currently in the public consultation phase. In addition to encouraging competition and investment in digital communications and commerce and enhancing confidence in digital transactions, the law has the specific goal of working to reduce the digital divide across the country and meet the needs of both individuals and institutions. Although the code does not deal specifically with ID systems, it does contain provisions to govern digital trust services more generally, including electronic signatures and certificates and encryption services, which are used for digital authentication and authorization for e-services and transactions.

Relevant parts of the code include, but are not limited to:[37]

- **Electronic documents:** Defined as those that consist of a set of letters, numbers, or other digital signals—including those exchanged by means of communication—which have content that can be understood and stored on an electronic holder that can be read and referenced when needed (Article 149). Electronic documents are considered official instruments if they are supported by a reliable digital signature (Article 151). In all cases where legislative or ordinal provisions require the preservation of paper documents, this requirement is fulfilled by using an e-archiving service. Furthermore, the electronic version of a paper document is considered an original copy and valid in the long term when it is created and saved using a service capable of electronic archiving. In this case, the original paper document may be destroyed, unless this conflicts with the legal provisions in force (Articles 181-184, see also Article 266).
- **Digital signatures:** Digital signatures will be accepted in place of written signatures and valid in court unless proven unreliable (Article 152, 160-161). If documents are signed electronically, a reliable method of identification must be used to ensure that the signature is linked to the electronic document associated with it (Article 149, see also Article 154-156 for more on reliability conditions).
- **Identity proofing for digital trust providers:** Before issuing certificates, digital trust providers will collect personally identifiable information through an in-person procedure on the basis of a valid authentic electronic signature certificate issued by the same or another authorized provider (Article 167).

37 This analysis is based on an unofficial and non-verified translation of the Arabic draft code by the authors.

- **Data security and oversight:** Information systems and networks of public agencies must have compulsory and periodic digital security audits by the National Agency for Digital Security. With the exception of the Ministries of National Defense, Interior and Local Development (that is, MALE), which the National Agency for Digital Safety will alert to complete an internal audit (Articles 209 and 210).
- **Once-only principle:** Public entities should not ask someone to give data that can be obtained remotely from other public entities. All public and personal data exchanged between public structures are the same as the legal authenticity of paper documents. In cases where the applicant has to send or deposit multiple copies of a single document, this requirement is considered to be satisfied in the case of an electronic document once a single copy of the document has been sent or deposited (Article 270).
- **Interoperability:** Public entities shall adopt the technical regulations necessary to ensure the exchange of data and documents without prejudice to their integrity or access to them (Article 275).

PART 3.
Building a Digital ID Ecosystem for Tunisia: Opportunities, Challenges, and Recommendations

The GoT has made a solid commitment to improving the identification of citizens as part of a broader strategy of digital transformation under the PNS. As Part 2 of this report demonstrates, the government has made significant progress in this regard, and Tunisia has the potential to become a regional leader in the identity space. At the same time, a number of gaps and challenges remain. This section summarizes the core **strengths**, **opportunities**, **weaknesses**, and **risks** of Tunisia's ongoing ID-related projects. It then makes a **series of recommendations** to help capitalize on its momentum and ensure that its ID systems meet the goals of the government and the Tunisian people.

1. Key Strengths and Opportunities

Foundational ID Systems with High Coverage

Tunisia has succeeded in building strong foundational ID systems—including the CR and CIN—which provide basic proof of identity for nearly the entire population. This is no small achievement and means that Tunisia is well on its way to meeting Sustainable Development Goal (SDG) target 16.9, to "provide legal identity for all, including birth registration" by 2030. In addition to coverage, the adoption of a computerized civil registration system (*Madania*) has greatly improved the accessibility of CR certificates to the population, increased the timeliness of vital statistics, streamlined many administrative procedures in municipalities, and enabled limited identity verification services for other public entities.

A Commitment to Building Digital Identity Infrastructure

As detailed above, the **GoT is currently implementing or planning multiple digital identity-related projects as part of—or related to—the PNS**, including the IUC, IS, social register, upgrading *Madania*, potential eCIN card, TunXRoad interoperability platform, TUNTRUST-based digital authentication and e-signatures, upgrading health information systems, and the CNAM smartcard. Many other PNS projects, such as online government portals and e-services, will rely on these systems for interoperability, digital authentication, and more. The involvement of multiple stakeholders and significant resources in these projects demonstrates significant commitment to—and demand for—developing a robust identity ecosystem as well as the strong technical capacity of multiple ministries.

The IUC System Incorporates Some Pro-Privacy and User-Control Designs

As currently envisioned, the IUC will be a back-end only number that cannot be stored in other databases or made public. **This design—which is articulated in the new LPDP—is intentionally meant to protect data privacy** by reducing the proliferation of a unique identifier across multiple systems, which can create certain data protection risks. Instead, the IUC will facilitate identity verification and interoperability by storing a mapping of the IUC to other sectoral identifiers in the central system only.[38] Furthermore, the IUC platform will include a portal for users to access and review their data, increasing individual oversight. If these designs are implemented well—along with other privacy- and security-enhancing measures—the Tunisian model may provide a new and innovative example for other countries to follow.

Significant Progress on the IUC, CR, and Social Protection Systems

In alignment with the PNS, the GoT has made **significant progress in a number of priority areas**. With regard to foundational ID systems, this includes progress on designing and beginning implementation of the IUC, as well as specifying and detailing an implementation plan to reform the *Madania* systems. Recently, a convention between MALE and MAS has also advanced the **planned mapping between the IUC and IS** and set out agreements for data exchange. Notably, plans for both of these systems represent progress toward meeting certain international norms, such as a **commitment to open standards and technology neutrality** and the architecture of both systems as **shared services and platforms** that can be leveraged across the government and **improve the interface between Tunisian citizens and the state**.

In terms of functional ID systems, the deployment and ongoing improvements to the IS represent a huge **advancement in sectoral interoperability and improving the identification of social fund beneficiaries**. Although the recent audit report has identified some ongoing challenges with the system, the CRES has developed a strategy to further improve the system. In addition, by registering beneficiaries for the noncontributory social programs (PNAFN and AMG1/2) and integrating this with the IS, the MAS has taken the **first steps toward building an integrated social registry** that could serve as a foundation for social protection within the country.

With regard to health insurance, plans to issue a basic 2D barcode card to CNAM beneficiaries will **enable digital authentication and improve the security and convenience of transactions** at a lower cost than alternative credentials (for example, a smartcard). Finally, by opting to extend issuing of the CNAM card to noncontributory health insurance holders (MAS beneficiaries), the GoT will help **prevent unnecessary costs** associated with developing a special credential just for these programs and **help protect the privacy of program beneficiaries** by not singling them out with a separate card. Should the country ever choose to implement a universal health care program, the CNAM card system could be relatively easily adapted to this purpose.

Clear Demand for Identification, Authentication, and Trust Services

In line with the priorities of the PNS, the potential demand for identification and authentication related services is high—across both public agencies and private companies seeking to digitize and streamline their processes, reduce fraud, and enable online services. This means that **investments in the IUC, sectoral registries, and digital authentication, and trust services will be highly valued, as long as they serve the needs of these potential users**. It also points to a number of opportunities to pilot the use of the IUC and potential authentication services in the near future, including in the following sectors:

38 In this way, it could operate similarly to a system that uses tokenization to limit the propagation of a unique identifier and stores the mapping of tokens to identifiers in a vault (for example, Austria)—see footnote 50 for more explanation.

- **e-government services.** A digital authentication platform is needed in order to allow citizens to securely log in to e-government services across a broad range of sectors, including health, education, social security and safety nets, taxation, and other administrative services.
- **Social protection.** Although the IS currently provides interoperability and efficiency within the social protection sector, mapping the IS to the RIUC database is critical to facilitate communication and data exchange with other sectors to further improve targeting performance using other administrative data to inform welfare level of households. In addition, certain social-sector transactions could benefit from a digital authentication infrastructure that provides a higher level of assurance.
- **Education.** As discussed above, there is currently a project to utilize the RIUC for school registration. If this system is successful, it will be scaled up to all private schools, this could facilitate the development of a unique registry of students that would be useful for improving school administration, including detecting school dropouts and managing scholarship programs, and help simplify procedures for parents and students.
- **Subsidy reform.** The GoT plans to design a cash transfer program to compensate for price increases resulting from the gradual removal of food and energy subsidies. Based on the current plan, the beneficiaries of this cash transfer will be identified using the IS and CIN, and other information such as a gas connection will be used for determining eligibility for the gas subsidy which will also require interoperability with the gas and electric company (STEG) database. Furthermore, a secure digital authentication system could be used to help reduce fraud and leakage during the distribution of cash payments.
- **Health.** As part of the ongoing project to modernize hospital information systems, it was decided in 2019 at a digital committee to the presidency of the government that the SI will be used in the health sector. Other opportunities to leverage the RIUC and/or digital authentication for health could also be considered.
- **Civil service reform.** The IUC could be mapped to the HR system and other back-end processes for civil servants in order to uniquely and accurately identify each employee. This could help ensure deduplication and the removal of ghosts, as well as consistent identification when civil servants move across departments.

By first adopting a multisector, medium- and long-term vision for Tunisia's digital identification and authentication infrastructure (see below), the GoT will be better able to vet such potential use cases and determine their desirability and feasibility.

2. Key Weaknesses and Risks

Uncertainties Around Project Accountability and Longer-Term Governance

Given the number of stakeholders involved in Tunisia's identity ecosystem (see table 1 and table 2) the authority and accountability for projects that reach across sectors are sometimes blurred. Beyond stakeholder coordination, **uncertainty still remains around the governance and administration of specific projects**. For the IUC, for example, while the overall role of the OGI has been defined, it has not yet been formalized through an implementing decree because of the delay in enacting the law on the protection of personal data (LPDP). In addition, **more consideration needs to be given to the change-management processes surrounding the IUC and other projects**, including the adaptation costs for various agencies and the training needs of civil servants.

Finally, the success of digitalizing identity, authentication, and public service delivery in Tunisia rests on the passage of the **LPDP and the digital code**. If these laws and their implementing decrees are not passed, it will put the aforementioned projects—as well as many projects in the PNS—in jeopardy.

Lack of a Coordinated, Holistic Vision for Tunisia's Identity Ecosystem

Although the PNS provides a big-picture view of the various projects and components needed to transform Tunisia into a digital society, there is **not yet a clear vision of how all of the identity-related projects—for example, the IUC, the IS, digital authentication solutions, TunXRoad, a unique portal for services, and so on—will work together that is shared by all stakeholders.** Although projects such as the IUC are governed by multistakeholder committees, interministerial collaboration appears to be on a project-by-project basis, with little crosscutting coordination. As a result, the sequencing (timing and dependence) of some projects has been difficult and created inefficiencies, and certain design decisions are being made ad hoc rather than with the big picture in mind.

Although significant progress has been made in defining the design of the IUC—for example, the initialization of the database and the recent MOUs signed between MALE, MAS, and the Ministry of Education, respectively—continued implementation of the IUC information system, the Madania redesign, and the national interoperability frameworks are crucial for realizing the benefits of these systems, as is the passage and implementing decrees of the LPDP and the digital code to solidify the role of the OGI and the IUC in the national-level identification and authentication ecosystems.

Limited Existing Solutions for Digital Authentication

Despite a push for digital government and e-services, **Tunisia currently lacks universally deployed or adopted digital ID credentials or platforms to enable secure online and in-person authentication.** The CIN card is the credential most used by adults as proof of identity, however this typically involves a simple visual inspection of the card and the person's photograph. In its current form, the CIN system does not offer the national infrastructure or levels of assurance needed for digital authentication either in person or online. In theory, the eCIN smartcard was meant to fill this gap, however the project has stalled and it is unclear whether the Ministry of Interior will continue this effort and, if so, in what form.

In the absence of the eCIN, **several other efforts and proposed projects involving the National Electronic Certification Agency (ANCE)39 have the potential to improve the country's authentication infrastructure** and meet the increasing demand for e-services:

- The most advanced solution is being developed by MTCEN and TUNTRUST: a server-side e-ID called DigiGO (remote Qualified Signature Creation Device)[40] and certificates on a cryptographic token (local Qualified Signature Creation Device). The DigiGO system will allow users to authenticate by providing a user name and password, as well as a one-time password (OTP) sent via SMS. In addition, TUNTRUST is currently working with MALE to implement the system for authenticating logins to municipal e-service portals (ongoing). These solutions can be used for digital authentication and e-signatures for various public and private services. However, the coverage and utilization is currently low: so far, 27,000 certificates have been issued by TUNTRUST on cryptographic tokens.
- TUNTRUST is also working on another proof of concept for a "citizen wallet" of stored primary documents (for example, driving license, diplomas, payroll slips, and so on) that could be used for authentication via a mobile app.
- There are also some initiatives at the CNI to work with telecommunication operators to identify citizens via mobile technology.

While these services have the potential to greatly improve digital authentication for e-services online, they do not (at present) solve the problem of secure in-person authentication, which is needed at least in the medium term, as most government services in Tunisia are still provided face-to-face. For example, the current primary method of in-person authentication is to physically examine the CIN card and compare it to the person. Although verifying the CIN number of a person (for example, via the RIUC) can help in establishing the accuracy of the information on the CIN card, it does not fully prevent identity fraud and offers a lower level of assurance than a solution that uses digital technology to securely authenticate.

Furthermore, there are some limitations to adopting only mobile ID solutions for online authentication in Tunisia. For example, the number of e-government online services is limited, and there is no requirement to use electronic certificates or strong authentication for other transactions. For the development of a digital authentication ecosystem, there is limited capacity in terms of registration and awareness for the services offered by TUNTRUST (for example, communication, training of field agents, and so on).[41] In addition, there are other limitations for deploying an authentication solution that uses mobile technology. Although mobile coverage in Tunisia is high, it is not yet 100 percent. Many people share mobile phones and the mobile operator's verification of identities is not 100 percent guaranteed, reducing the potential inclusivity (and security) of mobile-only solutions. Ideally, Tunisians should have multiple authentication channels, providers, and levels of assurance to choose from to maximize accessibility and usability.

---

39 TUNTRUST currently offers a number of digital certificate and e-signature services—including certificates for the TUNEPS government procurement system, electronic tax filing (e-Jebaya system), e-CNSS, CCPnet, electronic signatures for documents, and more. These services generally utilize physical (hard) tokens, which has limited their use; however, TUNTRUST is exploring the possibility of enterprise users storing the certificates on their own servers or hosting them on the TUNTRUST server. For a list of these services, see http://www.certification.tn/fr/nos-produits/id-trust-certificat-dauthentification-et-de-signature and http://www.certification.tn/fr/nos-produits/cachet-electronique-visible-tn-cev-2d-doc.

40 This electronic identifier is stored on the TUNTRUST server and the user can access the services using the connection ID, password and OTP protocol on their phone. The certificate stores the hashed CIN of the certificate holder for personal data protection. A copy of the CIN card is provided by the certificate applicant during a face-to-face interview with a TUNTRUST agent to ascertain the identity of the applicant. For more information, see https://www.tuntrust.tn/fr/content/digigo.

41 However, an agreement has been signed with ANCE and a private company to be a delegated registration authority (https://www.tuntrust.tn/fr/content/autorites-denregistration-deleguees), which should facilitate onboarding for the DigiGo solution via online face-to-face video. This solution will be operational after the Manage PKI platform is implemented (first quarter 2020).

Known Issues with Data Quality and Accuracy

A number of Tunisia's ID systems have **ongoing challenges with the quality and accuracy of their data**, as discussed throughout this report and summarized in table 16.

Table 16. Issues with Data Quality and Accuracy in Key Systems

System	Challenges
Civil Register (Madania system)	• Difficulties separating name chains in Arabic • Discrepancies between Arabic and Latinized names • Birth date errors • Multiple registrations of the same civil act (birth, marriage, and divorce) • Delays in updating the system for late births and vital events recorded abroad • Transcription errors of the civil act number, which does not include checksums • The databases for different events (births, marriages, and deaths) are currently separate, which introduces more possibilities for errors and duplicates
National ID (CIN)	• Legally, citizens are required to update their CIN with any changes in information. However, because the card never expires, many only reapply if their card is lost. As a result, certain data fields such as address and occupation are frequently out of date. • In addition, it is possible for people have multiple CIN cards/numbers or for multiple people to have the same CIN number.
Unique citizen identifier (IUC)	• During the initialization of the RIUC, errors detected between Madania and the CIN will be reconciled separately (either technically or via a data reliability campaign against the civil registry data, which will require a considerable effort with the help of the Ministry of Justice). • It must be ensured that client information system of the RIUC (currently MAS and Ministry of Education) respect the established protocol so as not to allow the creation of a functional identifier without going through an audit with the RIUC and the creation of a mapping between the two.
Social identifier (IS)	• Not all data from the CNRPS and CNSS migrated to the CRES database was accurate. • Some beneficiaries cannot be issued with an IS because their records lack the eight criteria used for deduplication. • The IS system is not directly linked with the Madania database, which is needed in order to ensure that information on beneficiaries is up to date (e.g., deaths, retirements, etc.); currently the funds validate the identity information of new enrollees using Madania, but they do not automatically receive updates when a beneficiary has died. • Married spouses who are both formally employed can independently enroll in the databases and may not be associated with each other.

There are currently plans underway to improve the accuracy of the Madania database, along with projects to increase interoperability with other ID systems and create family clusters, as well as the IS database. In both the short and long term, it will be vital to ensure the accuracy and quality of data stored in the Madania system, as the development and integrity of both the IUC and IS systems will depend on data from the civil register.

Low Interoperability and Continued Duplication of Data Collection

Although most identity databases in Tunisia are digital, **the level of integration and interoperability is low**. Even in the social sector—where the IS facilitates data exchange—agencies or programs (including CNSS, CNRPS, CNAM, and MAS) currently collect information for their beneficiaries separately and create distinct databases to implement their programs and services. As a result, there is often **significant overlap in identity records, creating redundancies and potential errors, as well as administrative inefficiencies when people transition from one program to another.** Implementing the ISU has helped reduce many of these issues, streamlining the verification of identities across systems. However, it has not reduced the redundancies in data collection activities, particularly for economic and social attributes that go beyond a person's basic identity. Duplicate data collection not only requires duplicate resources and has the potential to create errors and discrepancies between systems, it can be a potential risk to data protection and privacy by overprocessing personal data unnecessarily.

Project Implementation and Legislative Delays Could Create New Challenges

Many of Tunisia's ongoing identity-related projects and the broader components of the digital transformation strategy laid out in the PNS are **mutually dependent and require the passage of the LPDP and Digital Code.** Delays in deploying foundational projects or passing key legislation and implementing decrees could limit project success. For example, the proposed TunXRoad platform is an essential backbone of data exchange across government agencies, and necessary for the IUC to reach its potential, as are improvements to the Madania system. In addition, digital authentication solutions with varying levels of assurance are needed to deploy e-services, manage access control for systems like the IUC, IS, and Madania, enable people to login to the IUC's citizen portal, and strengthen the security of in-person services like opening a bank or mobile phone account. Delays in implementing foundational digital authentication solutions could therefore stall these services, or lead to a proliferation of sector-specific, siloed digital ID systems that are not interoperable.

3. Recommendations

Establish a Multistakeholder Committee to Synchronize Projects and Provide a Holistic Vision for the Future of ID in Tunisia

In order to improve coordination and achieve the additional recommendations below, **the GoT should convene a broad group of stakeholders for the ongoing ID and authentication projects.** This could be done under the leadership of MTCEN and MALE and include—at a minimum—all other stakeholders detailed in tables 1 and 2 (that is, CNI, ANCE, INPDP, Technical Police, Ministry of Interior, MAS, CRES, CNRPS, CNSS, CNAM, Ministry of Finance, ISIE, UAE, and so on), government bodies that are potential users of ID systems (for example, Ministries of Health, Education, Higher Education, and others), local governments, the private sector (for example, banks and mobile operators), and representatives from civil society. The initial goals of this exercise would be to:

- Ensure that all participants are aware of the status and plans for all ongoing initiatives and can relate these to other ongoing projects (for example, e-services, administrative reforms, Maison de service, and so on)
- Provide an opportunity for input and collaboration on the utility of these projects from different perspectives, and to consider additional areas of cooperation
- Find new mechanisms to ensure continued input and optimization of ID projects so that they meet the needs of different sectors and of citizens
- Determine how to better ensure clear lines of accountability for each project while maintaining cooperative and multisectoral projects
- Ensure that the resources are committed to train and support officials and various other users during implementation of new systems in order to ensure a smooth change-management process

In addition—and complementing the broad vision for a digital Tunisia offered by the PNS—this stakeholder group should **work to define a more specific medium-to-long term vision related to identification and authentication infrastructure.** For example:

- What should digital identity "look like" in five or ten years from the perspective of: (1) ID providers (for example, MALE, OGI, ANCE, Technical Police, and so on); (2) different government agencies (for example, social, health, education, tax, electoral administration, and so on); (3) citizens; and (4) the private sector?
- How can improved unique identification, interoperability, and authentication meet broader goals, such as building trust in government, increasing the capacity and innovation of service providers, and improving inclusive development?
- What will a person's interaction with ID systems ideally be throughout the normal course of their life, from birth to death?
- How will Tunisia ensure that people have meaningful choice, control, and oversight of their identity data, in accordance with international norms?
- How will each of the existing projects meet the above vision? What gaps or concerns still need to be addressed? Do they require new projects or a revision of current systems? Can projects and technological choices be better harmonized to improve efficiency and sustainability?

Beyond these broad issues, a multistakeholder group should be consulted in the pursuit of the subsequent recommendations. In addition, the lines of accountability for implementing this vision, as well as individual product components should be clearly defined and understood by all parties.

Ensure IUC Design Will Result in a Trusted, Inclusive, and Useful System

When leveraged by different sectors, a unique ID register like the RIUC has the ability to help service providers improve the back-end processes they use to identify citizens, beneficiaries and customers, reducing fraud and increasing efficiency. In addition, it can also help facilitate new modes of service delivery and simplify front-end administrative procedures for individuals.

In order to play this role, however, the IUC must be inclusive (cover the entire population), trusted (be reliable, secure, and accountable), and designed to add value for people and institutions.

As described in Part 2, table 13, the IUC system already plans to roll out a number of services on a pilot basis. It is recommended that the GoT build on this framework by identifying both a long-term vision and sector-specific plans for how the IUC can be leveraged and integrated into different sectoral systems and processes.

Table 17. Potential Benefits of a Unique Identity Registry for Service Delivery

Category	Benefits
Administrative efficiency	When **mapped to sectoral identifiers**—e.g., for social protection, tax, etc.—unique identifiers can automate identity queries, reducing time, labor, and the potential for human error. This includes automating: • Verification of basic identity attributes against the unique identity database (e.g., confirming the birth date of a new beneficiary) • Data exchange and queries between functional databases (e.g., checking the property register records for a taxpayer)
Fraud reduction and improved targeting	By **establishing uniqueness and facilitating interoperability**, unique identity can be leveraged by multiple sectors to reduce inclusion and exclusion errors: • Requiring a verified unique identity for new enrollees can weed out duplicates • Up-to-date information on deaths provided by links to the civil register can help eliminate ghosts • Data exchange across different sectoral databases—e.g., the tax administration and social security—can increase information available to make eligibility decisions about a person
User friendly services	If the back-end utilization of the unique identity is also **used to simplify front-end processes**, this can improve user convenience by: • Reducing the number of documents needed to enroll in a program or verify identity (e.g., for the CIN, a person needs to present a birth certificate, certificate of nationality, certificate of employment, etc.).

For each sector and potential priority use cases such **as e-governance, social protection, subsidy reform, health, and education, civil service,** stakeholders could **assess potential benefits across three categories, as shown in Table 17**, considering the following:

- How could the RIUC be used to (a) improve administrative efficiency and (b) reduce fraud and improve targeting?
- How can back-end improvements using the RIUC also be translated into more user friendly services for citizens (for example, by eliminating the need for them to bring physical copies of documents like birth certificates when enrolling in a program)?
- Which laws and/or government decrees need to be altered or updated to facilitate these new modes of service delivery?
- What resources need to be committed for different sectors to utilize the RIUC (that is, for necessary system updates, integration, training, business process reengineering, and so on)?
- More broadly, stakeholders should also consider:
    - Whether e-services will be available through a single government portal, and/or if each ministry will operate its own portal.
    - Whether an e-service platform will be the same portal through which citizens access records of who has used their identity information (as required by the IUC legal framework).
    - Whether RIUC verification services will eventually be available to the private sector (for example, to fulfill KYC requirements for banks).

With this vision and these use-cases in mind, the GoT should continue to **build the IUC in a way that is responsive to the needs of sectoral users and the Tunisian people, inclusive of the entire population, and trusted by individuals and institutions.** Key issues to consider include:

- How to include the small percentage of citizens who were never registered at birth (for example, most likely those in rural areas)?
- How to eventually include noncitizens?
- The governance structure of OGI—To whom will it report? How will it be administered? How will it be funded?
- What role will the IUC play in TunXRoad? Will the RIUC facilitate queries between different databases (for example, if the tax administration needs to request information from MAS)?
- How will the IUC be mapped to other existing identifiers (for example, for tax administration)?
- How will the IUC be mapped to databases that do not yet have identifiers (for example, hospitals, schools)?
- Who will provide the resources for users of the system—for example, MAS, Ministry of Health, Education, Finance, and so on—to adapt and/or digitize their databases to utilize the interoperability framework?
- What change-management processes will be adopted to ensure that both officials and citizens have knowledge of the new system and are incentivized to comply with it?
- What grievance redressal mechanisms will be adopted to ensure that all citizens—including those who are unlikely to have access to an online portal—are able to register complaints and easily correct errors with their data or its use?

Prioritize Reforms to the Civil Register and the National Interoperability Framework

Improvements to the civil register and the implementation of a national interoperability framework are crucial enablers of the RIUC and other identity-related projects and services. Strengthening the quality and utility of the civil register is a foundational ingredient in ensuring an inclusive and trusted identity ecosystem. In addition, the national interoperability project—called TunXRoad and supported by MTCEN—is a core goal of the PNS, and essential for ensuring that the IUC can be leveraged broadly across the public sector.[42]

As discussed in Part 2, MALE has already developed a strategy to improve the quality and accuracy of data in the Madania system in support of the RIUC, as well as the development of family clusters. In addition, this strategy also includes upgrading the system design to make it more reliable, secure, interoperable, and useful for different agencies, including the Ministry of Health, Ministry of Foreign Affairs, Ministry of Justice, and the INS. Continued progress and commitment to these efforts are essential to ensuring the quality and integrity of Tunisia's ID systems.

Accelerate Development of Digital Authentication Solutions

As described above, a number of authentication-related projects are currently underway, at different stages of development. **However, more holistic thinking is needed** to ensure that planned authentication systems: (a) meet the needs of various users and future types of transactions, including providing appropriate levels of assurance; (b) are cost effective and interoperable; and (c) are accessible by the broader population. In particular, **a multistakeholder group (as described above) should consider:**

- How current processes of authenticating citizens for in-person transactions could be improved in terms of efficiency, security, and convenience
- The immediate and planned needs regarding online authentication (for example, for e-services) across different segments of the population
- Which levels of assurance are needed for different types of transactions, in line with international best practices
- The advantages and disadvantages of different types of credentials and authentication mechanisms (for example, cards, cloud-based, mobile, tokens, and so on) with regard to: (1) accessibility for a majority of the population; (2) security and levels of assurance; (3) and cost
- How different solutions for digital authentication (for example, DigiGO, a potential eID card, private sector solutions, and so on) will interoperate and/or establish a federation of digital identity providers
- How to build authentication systems with appropriate "privacy-by-design" measures to ensure user control and data protection (see later recommendation)
- How digital authentication can be leveraged by, or related to, potential e-payments for various government-to-person cash transfers

42 To our knowledge, this interoperability layer will be modeled after the Estonian X-Road system (https://e-estonia.com/solutions/interoperability-services/x-road/), but it is not clear how closely it will follow its design. The X-Road system underpins Estonia's digital identity and e-government services by facilitating queries and data transfer across databases. Using a unique identifier (the PIC, or personal identification code) issued to every resident as a key, the X-Road system links hundreds of public and private systems that each maintain their own sovereignty, and exchange data and queries based on prespecified agreements. One notable feature of the system is that, under Estonian law, no database connected to X-Road is allowed to collect identity information that is already contained in one of the connected databases—as this information is available through the interoperability layer—eliminating duplicate data collection.

- Whether government-provided digital ID solutions can be used by the private sector (for example, for eKYC), which will often be a primary user of digital authentication and will drive uptake
- How to expand the ecosystem of potential digital ID and authentication providers, including the private sector

Notably, and unlike unique ID number schemes like India's Aadhaar, **the IUC as it is currently designed cannot be used as an identifier for online, cardless authentication.** Unlike the CIN number, the draft LPDP forbids the IUC number from being made public or printed on credentials, meaning that citizens will never know or see their number. In theory, however, an ID provider (for example, MALE, the OGI, or the ANCE) could tokenize the IUC—that is, replace the IUC with a randomly generated number unlinked to the IUC—and provide these tokens to citizens without compromising the secrecy of the IUC.[43] In order to leverage this tokenized IUC number as an identifier for authentication, however, people would still need to register to receive the number and be issued with credentials/authentication factors—for example, cards, passwords, PINs, biometrics, and so on—to prove their identity online.

Strengthen Sectoral Information Systems and Registries while Planning for Integration with National Systems

In order to take advantage of the IUC, digital authentication and TunXRoad, existing programs and services will need to **develop digitized, interoperable back-end systems.**

In some cases, such as health, where centralized registers of users (that is, patients) do not already exist, significant investment is needed to develop information systems and other infrastructure needed to connect with the national platforms and create e-services that can use digital authentication and trust services. In other cases, such as the social protection programs, there is already a well-developed system with sectoral interoperability facilitated by the IS (see Box 4 for more detail recommendations for the social protection sector). Even in the latter case, however, both planning and investment are needed to integrate existing systems with the IUC and TunXRoad in the future. In some cases—for example, the IS—agencies have found it necessary to develop parallel systems to serve immediate needs before the national platforms have developed. As much as possible, however, any short-term solutions should be designed with the long-term vision in mind to ensure future interoperability and avoid duplicative investments.

Box 4. Strengthening Social Protection Systems – Towards an Integrated Social Registry

To strengthen social protection systems, recommended key next steps are summarized below.

Improve the data quality (social identifier). While the social identifier IS is assigned to 10 million records, there are still data quality issues to be addressed in terms of the uniqueness of identities and consistency of information across different databases. A recent assessment[a] identified a number of action plans which highlight the importance of institutional arrangements and a closer coordination and a concerted effort among all stakeholders.

Expand the coverage of the registry. Currently, the MAS's beneficiary registry consists of 20 percent of the population (about 600,000 households). Beyond the current beneficiaries of the main social protection programs, it is recommended that the coverage to be extended to other programs and a larger number of potential beneficiaries, moving towards an Integrated Social Registry (see below).

43 Tokenization is a process of pseudonymization, which involves taking a sensitive identifier (for example, a unique ID or credit card number) an applying an algorithm to map it to a new identifier that is not sensitive (called a "token"). If the token becomes compromised (for example, the identity is stolen), it would be computationally unfeasible for the thief to reverse-engineer the true ID number, and the identity provider can simply issue a new token.

Operationalize a new targeting approach. Building on the new social protection law—which stipulates the use of scores and objective criteria to assess potential beneficiaries—the government needs to officially approve the new targeting approach to start its operationalization in selecting and assessing beneficiaries of social protection programs. In parallel, other business process and information systems need to be implemented to support beneficiary monitoring, payment, and grievance handling, and so on.

An **Integrated Social Registry (ISR)** is a system that provides a common source of information on both existing and potential beneficiaries of multiple programs and/or services. Using parameters unique to each particular social assistance or other social program, administrators can simply query the ISR to obtain data for people who match their specific eligibility criteria. In other words, different programs and services do not need to collect new data to select their beneficiaries. This can improve efficiency, generate financial savings, and reduce the burden on individuals by eliminating duplicative, expensive, and time-consuming efforts to collect, verify, and manage data. When combined with an interoperability platform that allows for data exchange and queries with other sectors (for example, tax, social security, land and property, registers, and so on), the efficiency gains can be even higher.

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

Protect Data and Privacy by Design

As discussed above, the overall architecture of the IUC system already includes some privacy-protecting designs (for example, limiting the distribution of the IUC and a user access portal), as do some of the planned upgrades to the Madania system (for example, encryption and enhanced security controls). In addition, the draft law on data protection (LPDP) sets out key parameters for the IUC and how it can be used, in addition to broader regulations on the processing of personal data by other government and private sector actors.

Compliance with these rules will be essential to ensuring success not only of the IUC, but also the collection, storage, use, and exchange of data inherent in other projects, including the IS, TunXRoad, and digital authentication solutions. This requires not only the continued oversight of the INPDP, but also a broader engagement with different government, private sector, and civil society actors to ensure that these regulations are fully understood and implemented.

Furthermore, and in compliance with the law, the GoT should also **work to implement additional operational and technical controls to ensure that data and privacy are protected by default** in any system that processes personal data, such as the IUC, *Madania*, the CIN, sectoral registries such as the IS, authentication solutions like DigiGo and the CNAM card, and more. Such measures include, but are not limited to, the strategies and solutions shown in table 18.[44] Furthermore, it is recommended that the GoT conduct **additional privacy impact assessments and threat-modeling exercises** to evaluate the impact and risks of current and future systems on the security of people's data.

44 See also World Bank. 2018. Privacy by Design: Current Practices in Estonia, India, and Austria. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/546691543847931842/Privacy-by-Design-Current-Practices-in-Estonia-India-and-Austria.

Table 18. Examples of Privacy-Enhancing Technologies and Operational Controls

	Strategy	Example Solutions (Not Exhaustive)
Data-oriented	**Minimize** the collection and processing of personal data to limit the impact on privacy of the system	• Collecting and sharing minimal data • Anonymization and use of pseudonyms when data is processed
	Hide personal data and their interrelationships from plain view to achieve unlinkability and unobservability, minimizing potential abuse	• Encrypt data when stored or in transit • End-to-end encryption • Key management/key obfuscation • Anonymization and use of pseudonyms or tokenization for data processing • "Zero semantics": randomly generated ID numbers (not sequential or significant) • Attribute-based credentials (ABCs)
	Separate, compartmentalize, or distribute the processing of personal data whenever possible to achieve purpose limitation and avoid the ability to make complete profiles of individuals	• Tokenization or pseudonimization by sector • Logical and physical data separation (e.g., of biographic versus biometrics) • Federated or decentralized verification
	Aggregate personal data to the highest level possible when processing to restrict the amount of personal data that remains	• Anonymize data using k-anonymity, differential privacy, and other techniques (e.g., aggregate data over time, reduce the granularity of location data, etc.)
Process-oriented	**Inform** individuals whenever their data is processed, for what purpose, and by which means	• Transaction notifications • Data breach notifications
	Give individuals tools to **control** the processing of their data and to implement data protection rights and improve the quality and accuracy of data	• User-centric identity services • Attribute-based credentials
	Enforce a privacy and data protection policy that complies with legal requirements	• Role-based access control with two-factor authentication • Remote access • Physical and cybersecurity measures
	Demonstrate compliance with the privacy policy and applicable legal requirements	• Tamper-proof logs • Audits

Source: Table adapted from the ID4D Practitioner's Guide (www.id4d.worldbank.org/guide). Original framework adapted from https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design to fit the ID system context.

Note: This table is meant to be illustrative of common privacy-enhancing technologies and operational controls, but it is not exhaustive.

id4d. worldbank.org

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP