ID4D
Digital ID Use Cases:
Lebanon

ID4D
IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP

Report No:

Mashreq
Mashreq Digital Dialogue & DD Watch

Lebanon Digital ID Use Cases

January 24, 2024

Digital Development Global Practice

THE WORLD BANK

1818 H Street NW, Washington DC 20433
Telephone: 202-473-1000; Internet: www.worldbank.org

Document of the World Bank

Contents

About ID4D

The World Bank's Identification for Development (ID4D) Initiative harnesses global and cross-sectoral knowledge, World Bank financing instruments, and partnerships to help countries realize the transformational potential of identification (ID) systems, including civil registration (CR). The aim is to enable all people to exercise their rights and access better services and economic opportunities in line with the Sustainable Development Goals.

ID4D operates across the World Bank with global practices and units working on digital development, social protection, health, financial inclusion, governance, gender, and data protection, among others. To ensure alignment with international good practices for maximizing development benefits and minimizing risks, ID4D is guided by the 10 Principles on Identification for Sustainable Development, which have been jointly developed and endorsed by the World Bank and over 30 global and regional organizations (see http://idprinciples.org).

ID4D makes this happen through its three work pillars:

1. Thought leadership, research, and analytics to generate evidence and fill knowledge gaps.
2. Global public goods and convening to develop and amplify good practices, foster collaboration across regional and global stakeholders, and support knowledge exchange.
3. Country and regional action through financial and technical assistance to realize inclusive and trusted ID and civil registration systems.

The work of ID4D is made possible through support from the Bill & Melinda Gates Foundation, the UK Government, The French Government, The Norwegian Agency for Development Cooperation (NORAD), and the Omidyar Network. To find out more about ID4D and access our other publications, visit https://id4d.worldbank.org/.

Acknowledgments

This report was authored by Adam Cooper and Christopher Tullis. It is the result of collaboration between the World Bank's Identification for Development (ID4D) Initiative and the Government of Lebanon. Excellent feedback and inputs were provided throughout the development of this report. We thank the following individuals (listed in alphabetical order) for their various contributions: Marie Louise Aboujaoude, Lina Abou Mrad, Imad Abou Rached, Georges Attieh, Georges Bechara, Ali Berro, Zeina Bou Harb, Dany Gedeon, Youmna Chacar Ghorayeb, Colonel Fadi Harb, Nasser Israoui, Bilal Kalash, Linda Kassem, General Elias El Khoury, Imad Kreidieh, Ziad Maadarani, Nisreen Mashmoushi, Charbel Nehme, Lina Oueidat, Her Excellency Minister Najla Riachi, Youssef Saad, Georges Saoud, and Amer Syagha (Government of Lebanon); Makram Bou Nassar, Najib Choucair, Pierre Kanaan, Ghada Sabbagh, Lynn Talouzian (Central Bank of Lebanon); and Farah Asfahani, Nay Constantine, Anna Corsi, Abdallah Jabbour, Mohamad Hussein Mansour, Harish Natarajan, Ahmet Fatih Ortakaya, Haneen Sayed, Ronald Eduardo Gomez Suarez, Tania Zaroubi, and Matt Zeller (World Bank). We also appreciate peer reviews by Julia Clark and Nadine Chehade.

Executive Summary

This report summarizes the findings of a series of World Bank Digital Development missions from November 2022 to July 2023 to Lebanon focused on priority use cases for digital ID and authentication services. It outlines how digital identity, as part of a wider digital transformation program, could significantly improve the implementation and delivery of public services in Lebanon.

Limitations of Current Identification Systems in Lebanon

The state of the legal identification landscape in Lebanon is explored in detail in the companion ID Diagnostic. As discussed in the Diagnostic, the civil registration system remains largely paper-based and thus is not, in its current state, a viable candidate for a digital identification system. The national identity (NID) card system, however, is digitalized, and serves as a potential foundation for digital ID. The main limitations of this system, as well as the other digitalized systems that are potential candidates for digital ID, are summarized below.

NID card

The NID card and database contain **outdated data** due to the: (a) lack of incentives for citizens to update their data (e.g., photo and name changes), impeding the Ministry of the Interior and Municipalities (MoIM)'s ability to fulfill its role as an authoritative source for such attributes, and (b) lack of interoperability with service providers who may have collected more recent data.

There are **few means of validating the NID's authenticity** due to the: (a) existing barcode being presently unusable for validation without a means to scan it, and (b) lack of a checking service or other verification service provided by MoIM.

There is **compromised trust for in-person transactions** due to: (a) outdated photos hampering the use of the ID to authenticate a cardholder's identity, and (b) the inability to validate ID card authenticity digitally, leading to overreliance on visual security features.

The NID card **cannot be used for online transactions** due to the: (a) lack of usable digital authentication functionality, (b) lack of support for electronic signature and managing digital certificates, and (c) missing link to complementary digital ID credentials designed for online use, e.g., a mobile ID.

Passport

The passport system is **irreconcilable with the unique NID** due to the: (a) lack of interoperability between passport and NID databases, although they are both managed by MoIM, and (b) lack of a checking service to correlate passport numbers with NID numbers.

There are **few means of validating the document's authenticity** due to the lack of a checking service or other verification service provided by MoIM.

Sectoral systems

There is a **potential for duplicate accounts** due to flaws in the existing ID systems used at onboarding. There is also an **inability to perform secure transactions** due to: (a) current financial service products not offering strong authentication or high trust, and (b) no cross-sectoral uniqueness, which impedes data sharing and interoperability across sectors.

Current Workarounds

In the absence of robust digital ID systems in Lebanon, sectors have resorted to exploiting various workaround solutions. While these workarounds allow parties to (partially) fulfill certain functionalities of digital ID systems, they remain inefficient, costly, and inadequate compared to a fully functioning digital ID system.

To create **unique identifiers**, workarounds include: (a) biographic deduplication based on attributes printed on the NID card, and (b) sector-specific "unique" identity schemes. To check **ID card validity**, workarounds include the assessment of visual security features, such as holograms, which presents various vulnerabilities, especially for online transactions. The **verification** of identity attributes can be accomplished only against the electoral registry, which does not contain complete or fully up-to-date data, since the NID database is not interoperable with other systems. To **authenticate** individuals, the photo printed on the card – which may be decades out of date – is the only option for identity verification in the absence of digital authentication.

Key Sectoral Use Cases for Digital ID

The table below summarizes the key use cases for digital ID across various governmental sectors, as well as the main challenges faced by sectors due to the limitations of the current foundational identification system in Lebanon.

Sector	Use case	Main challenges of sectoral initiative
Financial	Remote Onboarding (eKYC)	Robust identity checks needed during the onboarding of new customers and opening of new accounts for existing customers.
Financial	Credit registry	No reliable way to uniquely identify individual credit histories, leading to errors in determining creditworthiness and compromising financial institutions' trust in the credit registry.
Financial	Access to Frozen Deposits Deposit insurance	No unique personal identifier associated with bank accounts, meaning there is no way to reliably associate an individual's financial accounts, both across and within financial institutions. A future deposit insurance and partial access to frozen deposits under the BDL's Circular 158 are both based on a per-person (as opposed to per-account) basis, and they will be highly vulnerable to fraud unless account holders can be uniquely identified.

Sector	Use case	Main challenges of sectoral initiative
Social protection	Social assistance (targeting)	It is impossible to verify eligibility for social payments by verifying data produced or managed by other sectors or ministries, due to lack of interoperability between key systems. Vulnerabilities include the ability to falsify self-declared eligibility data, necessitating a costly additional in-person verification.
Social protection	Social assistance (registration)	Online registration processes operate without a trusted identity verification process or unique ID in place, opening the potential for fraudulent and duplicate registrations. Vulnerabilities include multiple registrations by an individual and double counting of household members.
Health	Medical records (data sharing)	Health centers are unable to share data on treatment, resulting in incomplete medical records, duplicate care, and treatment decisions made based on incomplete information.
Health	Medical records (creation)	The in-person onboarding required during the creation of a medical record requires the patient to have her medical record created as an additional step before treatment, or else receive treatment at a medical center that also offers an onboarding service.
Health	Medical records (access)	Patients do not have access to their medical records. Making such information available based on current systems would be an unacceptable privacy risk, as it is not possible to securely manage access to the health records.
Health	Visa process Medical insurance claims	The process for verifying the eligibility of medical claims for reimbursement is paper-based, in particular medical visas. This leads to inefficiencies and is a barrier to moving insurance reimbursement online.
Health	Remote medical consultations	Doctors are unable to verify the identity of patients during a remote consultation, and key process elements such as gaining access to a patient's medical record, cannot be done remotely.
Health	Tracking medications	The MediTrack system for prescriptions and payments for medicines lacks a unique identifier for patients across all medical systems, making it difficult to create a single, encompassing view of patient records, and complicating the effort to reduce duplicates.

Sector	Use case	Main challenges of sectoral initiative
Commercial	Real estate	There is no link between the NID number and land registration, although the land registration database includes a data field for the NID number. A previous analysis of 100,000 land ownership records against the NID card database could only confirm the property owners' identity in approximately two-thirds of cases.
Commercial	Commercial register	The commercial register requires the in-person presentation of NID cards or passports of the company's responsible officers. Verification of these key documents is manual and time-consuming. Lack of digital validation and verification leaves the commercial registry vulnerable to fraud based on multiple registrations and association with fictitious directors.
Public administration	Civil servants' registry	Utilizing the NID number as the primary identifier in the Civil Servants' Registry could reduce administrative overhead, duplicate wage payments, improve integration to tax systems, and make it simpler for civil servants to change jobs and start new positions.
Public administration	Tax	There is inadequate assurance of the uniqueness of the tax identification number (TIN) due to the lack of ID verification of physical persons (against the NID) and legal persons (against the commercial registry).
Public Administration	Civil status records	The civil registry is not fully digitized, and the existing digital civil status records are not interoperable with the NID card database. This prevents the verification of identity attributes, such as name (including spelling and name order) and date of birth on the NID card, against this authoritative source.
Public Administration	Biometric passports	The NID card is often used for verification of identity and eligibility for a passport application. There is no interoperability between the NID card database and other services, meaning that access to a verification service provided by the NID card system is not available.
Public Administration	Address database	Lebanon lacks a single authoritative source for residential address data. Address data gathered for the purpose of NID card registration is often outdated as there is no requirement to update data. Consequently, many Lebanese citizens' address records remain outdated.
Public Administration	Electoral lists	The Lebanese electorate continues to expand as many expatriates become eligible voters. In addition, there are concerns regarding voter fraud and misidentification at polling stations. Digitally verifying identity could play a significant role in preventing voter fraud, limiting misidentification, and accommodating the increasing Lebanese voter population.

Functionalities Required to Enable Sectoral Use Cases

The following section lists the various functionalities that need to be integrated in the foundational identification systems in Lebanon to allow authorities to adequately support the sectoral use cases listed above.

Civil registry

- Implement comprehensive legal reforms to allow full digitalization.
- Devise a strategy and timeline to progressively phase out reliance on paper registers for transactions.
- Implement unique NID number attribution from birth to allow lifelong identification.
- Implement interoperability with the NID system, including dynamic updating (sync).

National ID card

- Implement checking services to validate card authenticity and verify key attributes.
- Implement interoperability with civil registry and passport databases.
- Introduce incentives to update NID records, in particular photos that reflect the cardholder's current age.

Digital ID

- Enable digital authentication, to digitally verify the identity of a person during a transaction, both in person and online.
- Implement electronic signatures, including strong binding to an identity to enable high-trust signatures.
- Create a true unique identifier to facilitate data sharing and prevent duplicate records, implemented alongside related systems and data governance reforms to facilitate adoption.
- Implement selective disclosure of attributes, particularly those considered sensitive.

Authoritative sources

- Governance framework identifying authoritative source for key attributes.
- Implement interoperability to facilitate dynamic updating of authoritative sources as data is updated (at non-authoritative sources) during service delivery.
- Implement an authoritative residential address database, as an authoritative source for address data, logically distinct from the NID database.

Data Sharing

- Data sharing gateway at whole-of-government level facilitating eligibility checks and other quality and efficiency improvements to services.
- Data governance framework implemented to govern authorized data exchange and reuse, based on adequate data protection and cybersecurity frameworks.
- Varied data sharing models supporting functionalities such as selective attribute disclosure, decentralized data sharing, consent-based sharing, and other privacy-preserving techniques.

Recommendations

The following recommendations have been identified as priority actions for the Lebanese government to consider when moving towards a digital ID system in Lebanon. A summary is provided below, and the full recommendations can be found in the body of this Report.

Quick Wins

Enable service providers to validate NID card using the existing bar code. Since the NID number is currently readable in plaintext in the barcode, the MoIM could provide a solution to relying parties that allows the authenticity of a NID card, including its biographic data, to be verified digitally.

Implement checking services to verify data from core authoritative sources. Enabling services across government to check the validity of official documents or identifiers against the authoritative source (e.g., NID card) will enable remote onboarding for digital services.

Leveraging the NID for unique identification. Attributing the NID to user accounts in core services (e.g., health) by first verifying the person's identity to a high level of certainty will increase trust when transacting across government.

Short Term

Conduct civil society consultations and end-user research to inform broader digital ID strategy. While the present analysis has focused on the limitations of current systems and the digital ID needs of various sectors, further work is needed to clarify citizens' needs, pain points, and concerns related to digital systems.

Establish interoperability between NID card and passport databases. The lack of interoperability between the NID and the passport databases means that if a person registers for a service using a passport, there is no way to verify if that same person is already registered with a NID number. This is a key pain point behind the proliferation of sectoral identifiers. A checking service that allows the correlation of passport document numbers and NID numbers could resolve this issue and increase uptake of the NID number as a unique identifier by service providers.

Identify authoritative sources of data. There are multiple data sources across governmental ministries and agencies that provide the backbone of current service delivery, including ID cards, passports, driving licenses, tax identification numbers, and health IDs. A clear designation of authoritative sources will address several concerns with the current ID ecosystem, including: (a) the proliferation of outdated data in official databases; (b) discrepancies in identity attributes and other data across governmental systems; and (c) the lack of a method to adjudicate which version of a person's data should be retained for official use when there is a discrepancy.

Develop data governance and data classification policies. If data sharing becomes more widely adopted, then underlying data governance will become ever more important, as will the ability to classify data based on its use and sensitivity. Drafting appropriate policies early in the implementation cycle is vital, as they will be instrumental in shaping any eventual architecture and service design.

Medium Term

Strengthen legal and institutional enablers for digital ID, including cybersecurity and data protection. The current legal environment underpinning digital ID in Lebanon demands thorough revisions to effectively facilitate the digitalization of both ID and CR systems, ensuring the security and protection of personal data. Essential amendments to the outdated civil registration law are imperative to streamline existing paper-based processes and adapt to digitalization. Furthermore, implementing regulation is necessary to fully operationalize the NID for citizens. The legal recognition of digitalized identity documentation hinges on the adoption of the implementing decree for e-signatures, which was submitted to the Council of Ministers in January 2024. Additionally, enacting a comprehensive data protection law with independent oversight and adopting comprehensive cybercrime legislation in accordance with international standards are crucial to establish trust in the ID system.

Improve the existing NID card provision as part of wider digital transformation. Suggested improvements include a comprehensive cleaning to recollect data that is of poor quality or out of date, as well as mechanisms to ensure that data is kept up to date in the future.

Develop multiple alternatives for digital identity to meet the needs of various user categories. The opportunity to issue a digital identity credential could be considered in cases where high-trust credentials are currently issued (e.g., ID cards and passports) as well as the opportunity for individuals who wish to receive a digital credential (e.g., a mobile ID). The design of multiple digital identity credentials to meet the needs of various user categories should be informed by a broader digital ID strategy and consultations with civil society, and feasibility studies and cost-benefit analyses should be conducted to analyze alternative delivery models for digital ID and inform a roadmap for implementation.

Increase trusted data sharing and user-centric control. Further efforts to create a wider, trusted data sharing architecture could be considered. Activities could include strengthening the legal, business, and operational elements of a wider trust framework to allow more government ministries and their services to accept trusted data from digital sources.

Provide support to relying parties for wider rollout of digital identity. Providing support to relying parties, ranging from guidance and training to implementation support and example code, will be important to lower the barriers to digital identity adoption.

Long Term/Strategic

Achieve legal equivalence of digital identity and electronic signatures. Electronic signatures already enjoy legal equivalence with wet signatures in Lebanon through Law 81-2018, but the latter is not yet implemented due to a lack of an appropriate regulatory framework. Implementing electronic signature legislation based on a robust digital ID system is a prerequisite for scaling the digital economy by extending trust to higher-value transactions.

Develop data sharing architecture for the whole of government. A whole-of-government approach and architecture for data sharing can be used to help overcome current issues, such as lack of interoperability, duplication of data across systems, lack of authoritative sources and differing registration processes and credentials.

Enable citizens to manage their own data. Error in governmental records can be reduced by enabling citizens to authenticate themselves using digital identity, and by allowing them to manage their personal data. Citizen-performed updates can be sent automatically to all ministries, thereby simplifying user interaction with government and ensuring data is accurate and up to date.

Implement a national population registry to complement existing systems. Implementing a population registry to help underpin existing systems and integrating limited additional foundational data (e.g., residency status) could help improve identification, provision of public services, statistical analysis, and policy planning.

Introduction

In November 2022, a World Bank Digital Development mission to Lebanon organized deep-dive technical discussions focused on priority use cases for digital identity (ID) and authentication services. This report summarizes findings from these discussions and outlines how digital identity, as part of a wider digital transformation program, could significantly improve the implementation and delivery of online public services.

This report analyzes each use case and makes note of potential opportunities to strengthen digital identity. In some instances, a quick win – such as utilizing the existing 2D barcode on the national ID (NID) card to reduce data entry issues – can be implemented with minimal change to existing services. In other cases, more comprehensive investments are required, such as the introduction of digital identity and e-signature technology. Such investments call for deeper analysis of existing systems and their target architectures.

In general, there is large potential for digital transformation across multiple sectors of the Lebanese Government and economy, much of which is dependent on the establishment of the foundational elements of a whole-of-government and whole-of-economy architecture, such as interoperability standards, data governance, secure data sharing (e.g., via Application Program Interfaces (APIs))[1], and reliable identity verification, as provided by digital identity and e-signature technology.

Legal Identification

Legal identification systems provide proof of legal identity and recognition before the law. Sometimes referred to as foundational identification systems, they serve as authoritative sources of identity information of citizens and residents for official purposes. In Lebanon, the principal legal ID systems are the civil registration system (known locally as the civil status system), and the national ID system (which manages the national ID card). Trust in the digital ID systems that will be discussed later in this report is reinforced through the robust linkage of digital identity credentials to an officially recognized source of legal identity attributes.

This section summarizes the findings of the Lebanon ID4D Diagnostic, the companion document to this Digital ID Use Case Report. The high-level summary focuses on the Diagnostic's findings related to legal ID that are relevant to the discussion on digital ID analyzed in this Report.

Overview

While the Lebanese individual civil status extract (ICSE), which is the equivalent of birth certificates in other countries, is examined at length in the companion Diagnostic, the present analysis looks primarily at the national ID (NID) system and the primary credential (NID card) issued from it. The two systems' current states differ in their level of digitalization, and thus in their suitability to serve as a basis for digital ID. The civil registration (CR) system, which issues the ICSE, is only partially digitalized, whereas the NID system is fully digitalized and uses deduplication to assure the uniqueness of individuals registered in the system. This, combined with the ability to verify an individual's identity using the national ID card, makes the NID the most suitable candidate for use as a foundation for digital ID.

1 An application programming interface (API) is a software intermediary that allows two applications to talk to each other.

When it launched in 1997, the Lebanese NID card was state-of-the-art, however, to this day, its overall design has not been updated. Thus, Lebanon's current version of the NID card is nearly identical to the one first issued over a quarter of a century ago. The only data added to the card since inception has been the blood group; however, Ministry of Interior and Municipalities (MoIM) officials are debating the inclusion of additional data, such as residential address and religion. These, however, are problematic data attributes for inclusion on a NID card, as residential address is known to change frequently and religious identification would raise privacy and safety concerns.

As it currently stands, the NID card system collects biometric data from applicants and, following deduplication, issues unique identification numbers that are then attributed to people for the rest of their lives. The NID card is mandatory for Lebanese citizens over the age of 15 (those under 15 can also apply for a NID card, but they do not provide biometrics). An estimated 4.4 million citizens have NID cards, although there are over 6 million records in the NID database; the latter figure includes records for lost and duplicate cards as well as for deceased persons, as there is no reliable process in place for removing these persons from the database. In 2021, an estimated 97 percent of the Lebanese population over 15 years of age had a NID card.[2] There is no expiry date on the card, and citizens are not obligated to update or renew their card. Consequently, the data stored in the NID database is often outdated. The issue of updating data is not limited to text fields: many cards have ID photos that are effectively unusable, e.g., many adult NID cards still contain childhood photos.

The existing Lebanese NID card includes a 2D barcode on the back that can be easily scanned with a commodity device, such as a mobile phone or tablet. Although it is not yet widely used for identity verification purposes, as it can only be decompressed using a proprietary algorithm, this barcode could be a key enabler of remote identity verification when onboarding to a future digital identity. The barcode contains the following data: first name, family name, place of birth registration, family number, issuance date, blood group (unencrypted), and two fingerprint images (encrypted). Expanding the barcode scanning capability would enable other governmental services to not only verify the validity of the NID card, but to also enable those services to access trusted data directly from the barcode, with the consent of the holder, thereby reducing the risk of data entry errors and streamlining the application process.

Furthermore, Lebanon uses the NID card for identity verification and eligibility for passport applications. Yet, currently, there is no interoperability between the NID card database and the passport database, even though both are managed in-house at MoIM. This means that direct access to verify the NID card is not available during passport application, limiting the MoIM's ability to verify the identity of passport applicants, and raising the risk that passports may be issued with fraudulent or erroneous identity information.

While a 2017 decree mandates the use of the NID number as a unique identifier for citizens by all government entities,[3] most ministries currently use their own identifier for an individual. Although there are potential benefits of using a unique identifier across government systems (increased efficiency, improved data accuracy, reduction of fraud and leakages), Lebanon's current cybersecurity environment must be improved before such linkage can take place. In addition, the adoption among service providers of the NID number as a unique identifier is hampered by the inability to correlate credentials other than the NID card, such as the passport, with the holder's underlying NID number. Another barrier to NID adoption is a perception that many fraudulent NID cards are in circulation; such perception can linger due to the lack of robust means of verifying the authenticity of the NID card or authenticating its holder. In most cases, the various identifiers deployed by line ministries for their sectoral needs lack robust assurance of uniqueness,

2 World Bank. ID4D Global Dataset - Volume 1 2021: Global ID Coverage Estimates (English). Washington, D.C.: World Bank Group. http://documents.worldbank.org/curated/en/099705012232226786/P176341032c1ef0b20adf10abad304425ef

3 Decree No. 168/2017 "Setting the Rules and Procedures for adopting a unified identification number for each citizen to be used before the public departments and agencies, municipalities and all public legal persons."

leading to some concerns of persons with duplicate identities, either within or across sectors. This situation limits the ability of service providers and ministries to identify individuals reliably and uniquely, as well as to share data on citizens between administrations or make use of data verification against other government data sets.

The existing NID card will need to be updated with credentials that not only reflect the identity of individuals more reliably with up-to-date information and images, but also support digital use cases and the addition of digital identity functionality.

Digital Identification

Overview

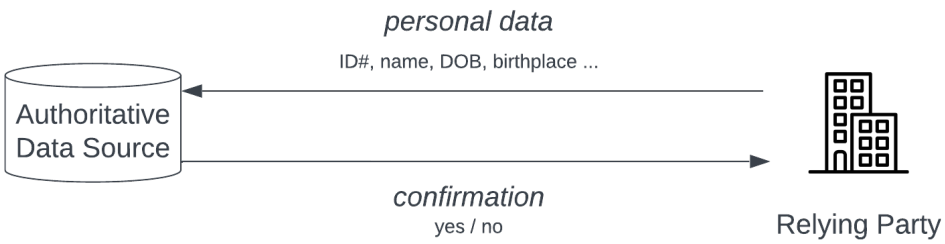
Digital ID Functionalities

The digital identification requirements for the various use cases will be analyzed in terms of relevance of the high-level digital identity functionalities below. For the purposes of this analysis, scope is limited to national-level digital identity systems.

1. **Unique identification** – If a person can assume multiple identities, it can threaten the integrity of identification efforts. One way to assure uniqueness within an identification scheme is to associate each person to a unique identifier (e.g., a number) for a person or entity. Current data protection best practice is to issue random identifiers, rather than logical identifiers that encode personal information, or to issue identifiers sequentially.

2. **Checking service –** A digital service that enables relying parties to request confirmation, in a yes/no response format, that an identity attribute or document is valid. An example might include an API that allows the verification of specific identity attributes (e.g., a name) or the confirmation of the validity of an identity document (e.g., a NID card).

Figure 1: Checking Service

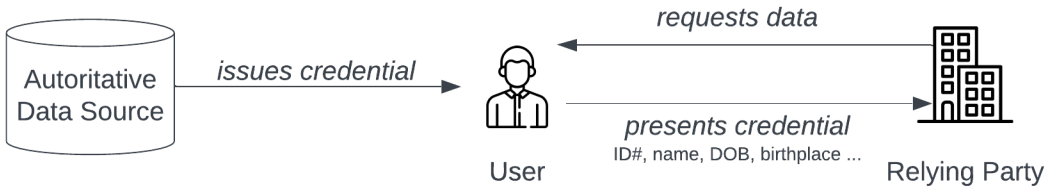


3. **Data sharing** – The ability to share personal attributes from an authoritative source (e.g., a NID system) with a relying party, under the consent and control of a data subject (the person). Trust may be assured though methods of verifying the provenance and integrity of the data received, such as a digital signature.

Figure 2: Data Sharing

4. **Digital credential** – A digitally verifiable means of proving claims made by an individual.[4] Digital credentials are a type of data sharing that puts the user at the center of the transaction. In the context of digital identification, digital credentials can be considered as the equivalent of a physical identity credential such as a national ID card.

Figure 3: Data Sharing with Digital Credentials



5. **Authentication** – The act of proving, at an appropriate level of trust, that the entity presenting a credential or other proof of identity is the entity to which it was issued. Authentication can be understood as a method of binding a person to an identity or credential for the purposes of a specific transaction.

6. **Electronic Signature** – A signature generated using digital means for the purpose of authenticating an electronic transaction.[5] While based on digital ID to identify and authenticate the signer, electronic signatures may offer additional assurances of integrity of the signed data and the signer's intent to be bound, in addition to preventing subsequent repudiation.[6] When generated in accordance with standards laid out in applicable legal and trust frameworks, electronic signatures enjoy the same legal recognition as traditional paper signatures.[7]

---

4 This is often manifested as cryptographic proof, such as a digitally signed credential issued under strict rules (e.g., a trust framework).

5 Christopher Tullis, Nay Constantine, and Adam Cooper (forthcoming), "Electronic Signatures: Enabling Trusted Digital Transformation," Digital Public Infrastructure Practitioner's Note Series, Washington, D.C.: World Bank Group.

6 Non-repudiation is defined as "protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message."
NIST SP 800-53. https://csrc.nist.gov/glossary/term/non_repudiation

7 In Lebanon, Law No. 81 Relating to Electronic Transactions and Personal Data provides for such a trust framework for legal recognition of electronic signatures, but the law has yet to be fully implemented.

The present analysis also integrates the concept of a level of trust, or level of assurance. The level of trust needed from a digital ID system is generally proportional to the risk level of the transactions or business processes it supports. Finally, the concept of a relying party is introduced.

- **Level of trust –** The level of trust, sometimes referred to as the level of assurance, is defined by processes under which identity or attribution of data to an entity has been achieved in accordance with recognized standards, alongside a means of ensuring the integrity and provenance of the data received.

- **Relying party –** An entity, often a service provider, that relies upon the credentials presented by a person, typically to process a transaction or grant access to a service. Depending on the type of transaction, relying parties may require different levels of trust in the credential issuer and the credentials themselves.8

Key Design Principles

This section outlines key design principles and good practices for digital ID, informing the recommendations outlined for Lebanon.

Identification systems

The Principles on Identification for Sustainable Development, consultatively agreed upon and endorsed by a broad range of public, private, and non-governmental stakeholders,[9] are firmly positioned to guide the implementation of digital identity infrastructure. Building on existing international norms for identification, the Principles were first developed and published in 2017 by a group of organizations[10] committed to supporting the development of identification systems that are inclusive, trusted, accountable, and used to enhance people's lives and the achievement of the Sustainable Development Goals (SDGs). The Principles are presented with their corresponding pillars in Table 1.

Table 1: Principles on Identification for Sustainable Development

PILLARS	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.

8 See, for example, NIST SP 800-73-4 under Relying Party. https://csrc.nist.gov/glossary/term/relying_party

9 Principles on Identification for Sustainable Development: Toward the Digital Age (English). http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age

10 From the public and private sectors, including NGOs, industry groups, the standards community, technology experts, and academia.

PILLARS	PRINCIPLES
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.

Data sharing

Using digital identity to enable verification and data sharing requires risk assessment for particular use cases and transactions. These risks can be reduced by implementing controls based on best practices used in other national-level digital identity systems. This report's methodology assumes the application of the following best practices:

1. **Checking services with a yes/no response should be favored over full data sharing.** Each use case must consider the need to use full data sharing (which can disclose personal data) over a basic checking service (which provides a simple yes/no confirmation). This consideration is particularly important when identity attributes, or other personal data, are in question. Checking services, which only share a binary response (yes/no) in lieu of personal data, can eliminate the need to share data in many use cases where only a simple identity check or eligibility check is required. For example, in the health sector, a checking service could be used to confirm eligibility for health insurance services. This approach provides an alternative to sharing sensitive health data, thereby reducing data overshare and consequently attacker attempts to collate sensitive data.

2. **Data sharing should have a clear purpose.** Where data sharing is necessary, the service design process must involve a full risk assessment and challenge the purpose for sharing data. Techniques such as checking services should be considered as an alternative to sharing data values. The service design process must also apply principles of data minimization and avoid data overcollection. Data governance frameworks should clarify the preconditions for sharing data, including creating provisions for securing transmission, avoiding oversharing, collecting consent, authenticating recipients, imposing limitations on data processing and retention, and providing sufficient audit and compliance controls.

3. **Data sharing services should be separated from production systems.** To minimize the risk of attack and to protect the normal operation of key governmental systems, data sharing services should be abstracted, or logically separated, from existing systems and infrastructure. Separation allows additional security measures to be applied to specific systems, isolates critical infrastructure from external services, and ensures additional pressure is not placed on existing services.

   From a security perspective, any data in such data sharing services can be not only encrypted but also secured from unauthorized access due to multiple layers of protection. System design can limit the type of data shared – for example, a checking service limits responses to yes/no – to reduce unintended or unauthorized disclosure. Services can be cycled and re-instantiated regularly (to reduce the risk of malicious code attack), and, in extreme circumstances, be isolated from external access entirely.

4. **Data should be encrypted at rest and in transit.** The integrity and confidentiality of data and messages are paramount. Data and messages should be digitally signed to ensure integrity. When at rest or in transit, sensitive or personally identifiable data should be encrypted to reduce the impact of potential breaches. Audit trails and other metadata should be subjected to the same controls.

5. **Monitoring and threat intelligence should be a priority.** All services should be monitored to alert operators to any potential security threat and to detect irregular behavior, such as changes in the normal operation of services or access to data. Equally, threat detection and threat intelligence tools should be used to preempt potential attacks and inform operators when reviewing service provision.

Detailed audit logs should also be maintained to enable monitoring of, and alerts about abnormal activity, and to act as a key resource in the event of an investigation. Logs should be tamper-resistant.

Potential to Support Digital Transformation

Modern digital transformation in Lebanon can succeed through the design and implementation of easily accessible services that offer real benefit to citizens. Digital identity is one element of the digital transformation stack, as it helps individuals reliably prove who they are to digital service providers, whether they are in the public or private sector. Digital identity goes hand in hand with trusted data sharing, enabled through interoperability, which provides for seamless exchange of information between entities. The combination of digital identity and trusted data sharing can increase efficiency, reduce fraud and leakages, and enable more effective and useful service delivery for citizens.

Most Lebanese governmental databases are siloed and often have no APIs or service integration options available, limiting their interoperability and ability to securely exchange data. In most cases where intergovernmental data exchange is required, data files are produced and shared as simple Microsoft Excel spreadsheets, and sometimes transmitted on media such as CD-ROM. These outdated data exchange methods carry obvious security risks and inefficient service delivery procedures, while lacking scalability and limiting the potential for digital transformation and integration across ministries.

Secure interoperability between governmental databases, which is needed to facilitate data exchange, is currently hampered by several factors: (i) the lack of a robust unique ID system that would facilitate the resolution of records across systems; (ii) the lack of accepted standards that facilitate data sharing; (iii) the lack of adequate data protection and cybersecurity measures to ensure data privacy; (iv) the lack of sectoral technical capacity to participate in such data exchange framework; and (v) the lack of a data governance regime that designates authoritative sources of data for any given attribute.

Introducing digital identity and mechanisms for authentication, alongside trusted data from multiple authoritative sources, would enable governmental agencies and the private sector to improve service delivery. Digital identity and its associated functions (e.g., identification, verification, authentication, e-signatures, data sharing, and attribution of data) can:

- **Increase trust and reduce risk** – Relying upon the NID number because, along with other identifiers, it has been verified as legitimately belonging to a person will immediately increase interoperability through common identifiers. Such reliance will also reduce transactional risk, as there is greater trust that individuals are authenticated (to include biometric authentication, as required). The ability to digitally verify information displayed on the NID credential, as well as to digitally confirm the validity of the credential itself, can also increase trust.

- **Increase efficiency** – Duplication often occurs due to weak identity verification methods or the inability to check against authoritative sources (e.g., passports and ID cards). Digital identity prevents account duplication and enables the identification and merger of existing duplicate accounts, by ensuring the occurrence of identity verification and providing the necessary trusted data and identifiers attributed to an individual.

- **Reduce fraud and error –** The individual citizen (person) is often in the best position to know if personal data (e.g., current address or email address) is accurate. Digital identity will increase the strength of individual authentication, providing greater trust in who is accessing or updating data. Such advancements will enable services to encourage individuals to keep their personal data current, while also making it difficult for fraudsters to access and exploit data held by governmental agencies or firms.

- **Enable mechanisms for consent** – Providing individuals with a means of documenting consent to use data for a particular purpose is an important safeguard against unauthorized data sharing and, depending on the use case, may be required for compliance with regulation. Collecting consent can also be an enabler of trusted data sharing, as this consent can be used to authorize the sharing of data across multiple ministries while maintaining compliance with data protection principles and legislation.

- **Enable interoperability at the personal level** – From an end user perspective, citizens will be able to have a more streamlined interaction with the whole of government. Changes to common data (e.g., a person's address or contact details) can be completed once rather than several times through multiple services. Furthermore, citizens can enjoy richer and more compelling services provided through digital platforms, as trust in a person's authenticity and their eligibility to access services can be based on trusted data shared across government.

A whole-of-society enterprise architecture and trust framework are needed to realize the full benefits of digital transformation, including technical aspects (interfaces, digital ID, consent services, digital signature), policy aspects (standards, authorization, access levels), security (physical security, transaction monitoring, access controls), legal and governance (institutional roles and responsibilities, data protection) and compliance (audit function, legal remedies). For example, a data sharing platform or API gateway could be implemented to facilitate secure access to checking services and specific purpose data sharing services between ministries' systems and new digital services supported by those ministries.

Once these elements are in place, existing systems, platforms, and frameworks (e.g., Dawlati), and sectoral initiatives (e.g., the commercial registry) can evolve and be onboarded onto the e-government data exchange framework once they are ready. Key stakeholders of these systems – including OMSAR and the Central Inspection – are open to evolving them in such a direction upon the emergence of a trust framework for e-government and interoperability.

Current Workarounds

In the absence of robust digital ID systems that implement the modern digital ID functionalities discussed above, Lebanese service providers have resorted to exploiting various workaround solutions. These various workarounds allow some limited assurance of elements such as the uniqueness of an identity, the validity of an ID card, the veracity of identity attributes, and the authentication of individuals' identity during transactions. The most common workarounds, summarized below, are suboptimal in terms of benefits provided, usability, robustness, security, and sometimes all the above. The need for such workarounds would be obviated through the implementation of robust digital identity systems.

Unique Identification

Biographic deduplication based on the NID card. Various sectoral systems in Lebanon – including those managing digital health records, financial credit registry, and social assistance transfers – have sought to reduce duplicate registrations through biographic deduplication based on attributes such as name, date of birth, and parents' names.

Although these methods of deduplication are helpful in identifying cases of accidental double registration, they are generally too weak to prevent deliberate fraud attempts. Biographic algorithms can be easily fooled by slight modifications to NID card data, as these algorithms often rely on manual data entry or, in some cases, on optical character recognition (OCR) based on NID card scans. In the absence of digital checking services for card validation and attribute verification, such modifications may go undetected.

Sector-specific identity schemes. In the absence of a reliable and verifiable national unique identifier, various sectors have taken to creating their own sectoral unique identifiers to fill the gap. The new Health ID project and the BDL banking identifier (used for the credit registry) are two such examples. In the absence of a national digital identity solution, additional siloed instances of "digital identity" will be created and, thus, risk creating a new wave of interoperability and usability issues for governmental agencies and the citizens they serve.

Checking Service

Visual security features. In the absence of a digital checking service that allows relying parties to confirm NID card validity, it is necessary to base the evaluation on the physical NID card. The NID card has a set of visual security features (e.g., etching and holograms) that were state-of-the-art in 1997 and still provide a reasonable level of physical security.

However, not all modern-day verifiers are adequately equipped to check these security features effectively, and in many cases, security features might not be checked at all. Even if they can be effectively verified, such security features only allow the determination that a card is genuine; it is not possible to confirm the ongoing validity of the card and check whether it has been revoked after issuance (e.g., after being reported lost or stolen). Additionally, since they must be evaluated in person, these visual security features cannot be used for remote transactions. Theoretically, the barcode could provide an additional layer of assurance of the validity of the NID card and the data printed on it; however, the barcode is never used in practice, as the algorithm needed to read it is not made available to service providers.

Verifying Identity Attributes

Verifying attributes against the electoral registry. While the MoIM's NID card and passport databases are not made available for identity verification due to security concerns, the MoIM's electoral registry is publicly available. The entire electoral registry can be obtained from MoIM on CD-ROM for a nominal fee ahead of each election, a measure that is designed to promote electoral transparency. Some service providers have reported buying this CD-ROM and using it to verify the biographic attributes provided by their beneficiaries. This workaround can provide an additional layer of assurance over relying entirely on the NID card, whose validity cannot be confirmed electronically. There are, however, several drawbacks to using the electoral registry this way, including: (a) the electoral registry includes the religion of each individual, which can lead to discrimination if made available to service providers for transactional use; (b) the list is updated only periodically, and thus will not include those who did not register to vote in the previous election, particularly young people who recently reached voting age; (c) the electoral registry does not include adults who choose not to vote; (d) until recently, diaspora populations were not included; and (e) other ineligible populations, such as the military and police, are not included.

Authentication

With no service in place to allow for the digital authentication of cardholders, service providers currently rely exclusively on a visual check of the photo printed on the NID card or passport for identity verification. This reliance presents a significant vulnerability, not only due to the complications of carrying out such visual checks for online transactions, but also because, in many cases, ID card photos are several decades old, and may no longer adequately resemble the cardholder. In extreme (but common) cases, NID cards of adults may feature a baby or childhood photo, making them useless for verification.

Digital ID Requirements Across Sectors

This section outlines the various needs for digital ID, and the corresponding functionalities that would be required, across different sectors.

Financial Sector

Customer onboarding

To onboard new banking customers and open new accounts for existing customers online, digital ID functions are needed to maintain integrity during the process, sometimes referred to as Know Your Customer (KYC), and to enable the process's digitalization (eKYC). This is required to comply with applicable Lebanese regulation as well as international requirements related to Anti-Money Laundering and Combatting the Financing of Terrorism (AML/CFT).[11]

Digital identity can enable high-trust remote onboarding for financial products and services, reduce the burden on citizens to produce paper evidence during onboarding, and lessen the overhead of application processing in financial institutions. Deploying remote client onboarding at scale requires an ability to verify attributes, such as identity and

11 Financial Action Task Force (adopted 2012, updated 2023), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation (The FATF Recommendations)".
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html

address, against authoritative data sources. Specifically, checking services can be used to confirm the validity of the ID credentials used for onboarding, as well as the identity attributes they contain, to avoid fraud and transcription errors. Alternatively, identity data could also be shared with financial institutions directly from the authoritative source. While such alternate workflow has the potential to improve efficiency and user experience, the additional data protection measure required could make a simple checking service a preferred option.

An additional requirement for remote account opening in Lebanon is an electronic signature to sign the application. The Central Bank of Lebanon (Banque du Liban, BDL) has recently issued a regulation to enable eKYC through e-signatures,[12] although implementation by financial institutions was still incomplete at the time of writing. While electronic signatures have broad applicability across the digital economy, the financial sector could anchor demand for e-signature services, shaping their development and eventually leading to adoption for other use cases and in different sectors.

Remote financial transactions

Digital ID and e-signatures also enable remote transactions. Although simple (low-trust) e-signatures can already be used for some relatively low-risk transactions (such as account opening, as discussed above), there are untapped opportunities to expand the usage of e-signature to increase trust in other types of financial transactions. Riskier and remote financial transactions – such as wire transfer orders and credit agreements – could also be implemented, but they may require higher-assurance e-signatures for trusted execution.[13] Strong digital authentication allows assurance of the client's identity during transactions and enables the implementation of the high-trust electronic signatures needed for high-risk transactions.

Credit registry

BDL operates a credit registry that contains information on individuals' accounts, outstanding debt, and other elements related to their risk profile. The registry is accessible by financial institutions that are subject to Lebanon's banking secrecy law for the purpose of allowing them to make informed credit decisions (for confidentiality reasons, non-bank financial institutions that do not engage in lending, or are not licensed by BDL, do not have access to the credit registry). Such credit registries have been shown to improve access to finance by providing evidence of customer ability to repay a loan, reducing the need for individuals to provide documentation of their creditworthiness that they may otherwise be unable to provide.

While BDL's credit registry contains records for approximately 1.5 million banking clients, the ability to assure uniqueness is limited in the absence of a means to uniquely identify banking clients across financial institutions.

The BDL credit registry assumes that individual profiles are uniquely identified. To assure this uniqueness, individuals must provide a copy of their NID card when they onboard to the credit registry. BDL's system uses the ID information to perform a biographic deduplication, providing some assurance that the same person is not registered twice.

However, there have been many instances of duplicate registrations detected, due to the system's inability to

12 See Intermediate Circular 667 on Electronic Banking and Financial Operations, updating Basic Decision 7548, accompanying Circular 69 of 7 June, 2023 accessible in Arabic at:
https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Basic%20Circulars/Decision_7548_AR%C2%A782_1.pdf

13 One future application could be for any deposit insurance scheme to make remote payouts to beneficiaries, as the large number of Lebanese expatriates in the pool of eligible beneficiaries may make it untenable to require all depositors to return to Lebanon to receive their benefits in person.

flawlessly validate the NID card and the attributes printed on it. One observed fraud vector has been to modify or falsify a NID card by changing one of the biographic attributes, such as the name of one of the parents of the ID card holder. Such an alteration is sufficient to fool the biographic deduplication process. To protect against this risk, BDL has used the electoral registry – which is public information provided by the MoIM on CD-ROM format – as an authoritative source to establish identity attributes. Since the electoral database is updated ahead of each election cycle with data from the NID card database, it can serve in this context as a proxy for the underlying authoritative data source.

While BDL's credit registry has been able to eliminate a number of duplicate entries using this workaround, there are several important weaknesses in this approach, namely: (a) the electoral registry is perpetually out-of-date, as it does not include updates made to the underlying NID database since the previous election; (b) it does not include those who are ineligible to vote (or eligible voters who chose not to vote); (c) it does not include non-citizens; (d) it does not include persons who were below voting age during the last election; (e) it does not cover certain populations that are ineligible to vote but still access financial services, such as the police and military.

All these weaknesses could be overcome, and the problem of duplication solved, if NID cards use at onboarding could be validated digitally, if the identity attributes input into the credit registry could be verified against an authoritative source of identity data using a secure checking method, and if the uniqueness of the credit registry could be assured through linkage with a robustly deduplicated ID system such as the NID system.

Deposit insurance and access to frozen deposits

Under BDL Circular 158 (issued June 8, 2021), Lebanese banking customers have limited access to their frozen USD deposits. The scheme caps access to funds at US$ 400 a month per individual, in addition to other requirements and restrictions.[14] Like the mooted deposit insurance scheme, Circular 158 is implemented on a per-individual, and not a per-account basis, and therefore requires a unique registry of banking customers.[15] BDL has created such a registry for participants in the Circular 158 scheme that contains over 135,000 unique depositors. However, the registry's inability to check the validity of identity documents with a sufficient degree of assurance—in particular, NID cards and passports—leaves it vulnerable to potential duplicate registrations and thus duplicate payouts.

Lebanon's current economic crisis is expected to cause significant restructuring to its financial sector. While the contours of the restructuring are not yet finalized, the final package is expected to include provisions for deposit insurance, particularly for small depositors. Financing for such deposit insurance schemes could entail an injection of public funds, including from international sources, such as the International Monetary Fund (IMF). For example, the IMF's staff-level agreement with the Lebanese government in April 2022 includes a prior action for "Cabinet approval of a bank restructuring strategy that recognizes and addresses upfront the large losses in the sector, while protecting small depositors and limiting recourse to public resources."[16]
Depending on how such deposit insurance schemes are designed, effective identification of account holders may be instrumental to effective implementation. For example, Lebanon is considering a scheme to insure deposits of up to US$ 100,000 per individual (although no official position has been reached in this regard), thereby protecting

14 Under a previous scheme, US$ 800 per month (or US$ 9600 per year) was accessible half in USD and half in LBP, with the LBP portion being subject to a significant haircut as the official exchange rate is used (the amount of the haircut varies with the black-market LBP/USD rate at the time of the withdrawal). In June 2023, circular 158 was revised to reflect the current scheme (at the time of writing), limiting withdrawals to US$ 400 for existing beneficiaries and US$ 300 for new beneficiaries. https://www.bdl.gov.lb/files/circulars/158_en.pdf

15 Because such a unique registry of banking customers entails a violation of Lebanon's banking secrecy legislation, individuals who wish to benefit from Circular 158 must consent to waiving their banking secrecy rights and being included in the registry as a pre-condition to accessing the program. https://www.bdl.gov.lb/laws/download/2/en

16 "IMF Reaches Staff-Level Agreement on Economic Policies with Lebanon for a Four-Year Extended Fund Facility" (Press Release).
https://www.imf.org/en/News/Articles/2022/04/07/pr22108-imf-reaches-agreement-on-economic-policies-with-lebanon-for-a-four-year-fund-facility

small depositors. If protection is per individual and not per account, it would be necessary to robustly and uniquely identify all account holders to determine which accounts would be eligible for a payout. Strong authentication of account holders would be needed to prove that a given individual requesting deposit insurance has not already been reimbursed for deposits held in a different account. Vulnerabilities in the identification scheme used could undermine trust in the deposit insurance scheme and open the door to high levels of insurance fraud, potentially reaching or even exceeding hundreds of millions of USD.

Maintaining trust in these processes requires the ability to identify duplicate claims through the deduplication of the list of accounts, by associating each account with the identity of a unique individual account holder. When claims are made, the unique identity of the account holder could be matched to the claims registry using a checking service, to ensure that a similar claim has not already been processed against another account.

Social Protection

Verifying eligibility for social assistance

Most ministries with social protection programs maintain their own beneficiary databases. Assuring the uniqueness of beneficiaries across these systems is important to prevent duplicate registrations and double dipping. Currently, as there is no reliable mechanism in place to assure beneficiary uniqueness, these systems are believed to contain some duplicates. The lack of interoperability with the national ID system, or the use of the Unique Identification Number (UIN) as a unique identifier across systems, precludes effective beneficiary deduplication and limits the ability to verify beneficiary data against multiple authoritative sources, making means-based targeting difficult.

Given this situation, there is high potential for other authoritative data sources to be identified across governmental systems, which could play an important role in simplifying the application process for eligible parties and reducing the level of fraud and error experienced in the future. Examples could include checking against the passport database at MoIM to determine if an individual travels extensively, or accessing the Ministry of Finance's database to check if household income is over a certain eligibility threshold. For data protection reasons, access to these data sources should be restricted to certain services and should avoid disclosing as much personal data as possible.

For example, a system could simply return a categorical 'yes' or 'no' to a specific question – such as determining if an individual travelled internationally more than three times in 12 months – to significantly reduce the need for data sharing while allowing the program's requirement for eligibility determination to be met.

Utilizing the NID system to enable trusted data sharing and digital identity verification would greatly improve data accuracy, reduce the risk of fraud, and provide faster and better-targeted services to those most in need of assistance from the state. Once identity has been verified and eligibility data acquired from the user, further eligibility data could be accessed from other government/authoritative sources. An example could be to check if a person owns valuable assets such as a car (checking service against the vehicle registration registry) or real estate (checking service against the cadastral registry).

Registration of social assistance beneficiaries

The World Bank-funded Emergency Social Safety Net (ESSN) program enrolled poor and vulnerable beneficiary households into the beneficiary registry ("DAEM Social Registry") using an online registration platform called DAEM.

During the ESSN application process, which closed after a fixed application window during the COVID-19 pandemic, applicants were asked to upload scans of their NID cards. The DAEM platform, which is not connected to the NID system, was not able to confirm the validity of these scanned documents or verify the corresponding identity attributes. Deduplication was thus performed using biographic data, opening the possibility for bad actors to duplicate registrations by falsifying one or more biographic data attributes on the scanned card image. To counter this risk, in-person visits were carried out by social workers to registered households to verify NID cards and gather additional relevant information, as well as by the World Food Programme to confirm eligibility.[17] These additional identity and eligibility verification measures added to program administration costs.[18]

In addition to household visits being expensive and time-consuming, they do not assure beneficiary uniqueness as effectively as would automatic verification using the NID system. Efforts have been made to link the DAEM Social Registry to the NID system, but they have yet to yield results. If ESSN is expanded to new beneficiaries in the future, robust mechanisms would need to be in place to validate the ID documents used during registration to prevent duplicate enrollments.

Further complicating the process, the ESSN beneficiaries had to be deduplicated against those benefitting from a legacy social assistance program called the National Poverty Targeting Program (NPTP), since the policy was that beneficiaries of the latter were not eligible for ESSN. Since the NPTP was not implemented using the DAEM Social Registry nor used the UIN as a unique identifier, deduplication entailed a tedious, manual, and error-prone process that took several months. During this time, benefits to otherwise eligible households were suspended and could not be redeemed.

A rapid improvement could be to utilize the NID card's barcode to reduce errors in data entry for the NID number. This could lead to additional verification checks should MoIM provide a checking service to verify the validity of the NID card and/or the identity attributes it contains. The ID number could then be used for duplication checks or to block multiple applications from the same ID number (previously used ID card), helping ensure uniqueness of the DAEM social registry.

Improved ID verification, coupled with interoperability with the registry of civil servants, would also help the ESSN program identify and prevent payments to public-sector workers, as these workers are not eligible for the program. Digital ID authentication, if implemented during registration to the social registry, could add extra assurance of beneficiaries' identity.

---

17 Eligibility is verified using a quantitative methodology called proxy means test (PMT), which is tailored to each context and the available data. In general, improved access to relevant shared data from authoritative sources can be expected to improve the quality of this targeting methodology.

18 There have been past efforts under the ESSN project to build interoperability between DAEM and MoIM to facilitate digital identity attribute verification and NID card validation, but capacity and budgetary constraints have hampered such efforts.

Health

Tracking of medication distribution

Created to track medicinal prescriptions and payments, the MediTrack system lacks a unique identifier across all medical systems, making it difficult to track demand for (and potential abuse of) certain medications. To address this issue, the planned introduction by the Ministry of Public Health of a Unique Patient Health ID that includes identity verification with a digital identity would improve trust in the identification of patients.

Widening the scope of MediTrack will depend in part on the trust in patient identification and in the integration of MediTrack with primary and secondary care systems. Interoperability standards and trusted data sharing systems will be vital for this increased interoperability to succeed, particularly because there are multiple healthcare system vendors in the ecosystem. The ability to uniquely identify patients against a deduplicated authoritative source such as the NID system will be critical to ensure that all medications are linked to the correct patient.

Medical visa processing and insurance claims

The process for verifying the eligibility of medical claims for reimbursement is paper-based, in particular for the creation of medical visas to facilitate secondary-care referrals (and subsequent treatment and insurance claims). The healthcare visa process involves a system that requires a family doctor (primary care) to initiate a healthcare visa that is then processed at a visa center before allowing a patient to be admitted and treated at a hospital (secondary care). An insurer may require such a referral to have been made as a condition for the reimbursement of claims. While cumbersome, such procedures can be useful for securing health records and controlling patient care, especially when all patient interaction is in person and all documentation is paper-based.

The digital transformation of this process, particularly at the visa processing centers, and the eventual reclamation of funds, would provide a better outcome for patients and considerably enhance the efficiency of the Ministry of Public Health. Digital identity could play a vital role in the digital transformation of the healthcare visa process by reducing the need for in-person visa processing and increasing certainty in patient identification. Electronic signatures could allow doctors to sign visas digitally and initiate them remotely, potentially obviating the need for an in-person primary care visit to authorize secondary care.

Electronic healthcare records

Patients in Lebanon do not have access to their medical data, and electronic healthcare records (eHR) are not yet available. The future emergence of eHR increases the need to correctly identify patients before giving access to records, as well as to identify the doctors accessing these records. This ensures that doctors are authorized to consult these records, and it allows the implementation of appropriate access controls and audit logs. It is also needed to ensure the continuity of medical records across facilities (e.g., if a person moves or changes doctors), providing for the portability of patient records and the continuity of treatment. Digital identity is likely to be an important enabler for eHR, as it could be used to facilitate data sharing with healthcare professionals and make data available to patients. Accessing medical records remotely by doctors could improve care, and opening them to patients could give patients transparency over their care and control over their data. However, in both cases, robust digital authentication is needed to ensure that only authorized persons have access to sensitive patient health data. Additionally, trusted data sharing systems are needed to protect the data in transit when shared (e.g., between hospitals). Other digital ID functions could be used to further improve trust in eHR; for example, digital authentication of health center staff creating and editing records could enable the creation of trusted audit logs to monitor unauthorized access and help prevent tampering.

Efforts to continue improving the provision of healthcare services to patients have explicitly recognized the unique identification of patients as a priority. Unique identification can reduce multiple and duplicate records being created and maintained across different healthcare settings (e.g., multiple hospitals), and facilitate matching up patients' records across hospitals. Additional benefits of unique identification include better analytics, reduced error and administrative overhead, and increased overall ability for practitioners to deliver appropriate care.

To achieve these goals, the Ministry of Public Health has initiated a Health ID project, which proposes a common, sector-specific identifier, and may later add digital ID functionality such as verification and authentication. In the absence of a national-level framework for digital identity, other siloed instances of "identity" will be created and, in doing so, will create a new wave of interoperability and usability issues for other Lebanese ministries and the citizens they serve.

Remote medical consultations

Doctors are currently unable to verify the identity of patients during a remote consultation, and key processes, such as obtaining access to a patient's medical record, cannot be done remotely. There is also a need to authenticate the identity of doctors conducting remote consultations. For example, a family doctor could conduct a remote consultation with a patient, with the session secured using digital ID verification, allowing a healthcare visa to be initiated and a visit to a specialist hospital authorized without the cost, delay, and inconvenience of a preliminary in-person consultation. The lack of trusted digital ID leads to inefficiencies and is a barrier to the implementation of telemedicine.

Commercial

Real estate

Land registration covers private and governmental real estate registrations, including title deeds, mapping, and surveys. The land registration office also provides support for legally binding transactions, such as proof of ownership when mortgaging a property.

The land registration system is aging in both design and infrastructure. Applying for land registration can be time-consuming due to the in-person requirements (e.g., providing documentary evidence to a notary public). Processes for verifying the identity of landowners are unreliable: according to the MoF, a previous analysis of 100,000 land ownership records against the NID card database could only confirm the property owner's identity in approximately two-thirds of cases, equivalent to 30 percent unverifiable registrations. There is no link between the NID number and land registration to enable automatic verification, despite widespread NID card adoption and the land registration database containing a data field for the NID number.

Digitalizing the land registration process presents an opportunity to reduce application processing time while increasing trust in the process, by enabling individuals to go online to complete the application, prove their identity, and potentially share trusted data. The increased utilization of electronic signatures could also help to raise trust in the land registration process and enable the issuance of official documents, such as land titles and mutation papers.

The digitalization of such processes is particularly relevant in Lebanon given the very large diaspora population, allowing property owners to manage their assets without travel.

Verification of identity is completed by notaries public, who use their own systems to process applications. There is no official, standardized method for notaries public to identify themselves in digital transactions, nor to reliably confirm their notarial authorization. Digital identity and e-signature may well play a role in increasing trust in these transactions.

Furthermore, the "lost deed" process includes posting notices in newspapers to identify possible claimants. An online land registration application process could utilize digital identity to enable online responses.

Due to the high value of most real estate transactions, high-assurance digital ID systems are needed to provide adequate trust to allow digitalization. Unique identification of the parties to a transaction allows for each property to be identified with its owner, preventing errors and fraud such as tax fraud or unauthorized sale. Digital authentication allows high assurance of the identity of parties to real estate transactions, allowing the latter to be conducted digitally or, potentially in some cases, remotely or online. High-trust electronic signatures could allow key real estate documents, such as property deeds and sales contracts, to be signed electronically.

Commercial register

The commercial register requires in-person presentation of NID cards or passports of the company partners or directors (responsible officers). The verification of these key documents is manual and time-consuming for both the responsible officers and the government officials performing verification. The inability to reliably validate ID documents, verify attributes, and authenticate responsible officers undermines trust in the commercial registry and introduces vulnerabilities (e.g., failing to identify companies registered to fictitious persons or listing fictitious directors).

Access to checking services linked to authoritative sources of ID data could substantially improve the reliability of these identity checks. It could also provide an opportunity to impose additional anti-fraud checks, such as checking civil (mortality) registers and lost or stolen document databases. The ability to uniquely identify principals and directors would further improve the ability to regulate and monitor commercial entities.

Digital identity could also potentially be used for access to a future digital service that allows individuals to authenticate, prove their identity, submit relevant company documents, and fully register a new business online in a fraction of the time currently experienced.

Public administration

Civil Servants' Registry

The Lebanese Civil Servants' Registry (which includes approximately 8,000 civil servants, 4,000 contractual employees, and 1,000 wage laborers) uses a system-specific identifier generated during registration, along with a Tax Identification Number. The system does not interoperate or have any direct link to the personnel systems of other ministries.

Assuring uniqueness in the Civil Servants' Registry, which could be done by uniquely identifying civil servants, could reduce duplicate or "ghost" workers and wage payments while reducing administrative overhead from manual identity cross-checks. This could be accomplished by associating each civil servant record with a unique ID record, such as a

national ID. An appropriate checking service made available by MoIM would allow this association to be carried out robustly. It would also make it simpler for civil servants to change jobs and start new positions.

Leveraging the NID, potentially coupled with digital authentication, could also facilitate the payment administration for civil servants directly on their accounts, particularly if it were integrated into a broader government-to-person (G2P) payment infrastructure.

Tax Registry

Taxpayers in Lebanon are identified by a Tax Identification Number (TIN). The TIN is issued by the Ministry of Finance (MoF) for both individuals and corporate entities. A tax identification card is issued to individuals, while a registration certificate is issued to corporate entities. To get a TIN, an individual or an entity must submit the appropriate taxpayer forms to the Ministry of Finance. Once the forms are approved, the individual or entity receives their TIN.

According to the MoF, over 90 percent of taxpayers declare and pay taxes online. To enroll, taxpayers must visit the MoF's website and complete an online registration form. Upon completing the form, taxpayers receive an email scheduling an appointment at the Ministry, where they are invited to submit their supporting documents in person, alongside the TIN identification card, and receive an e-PIN number enclosed in an envelope that allows access to the online tax system.

The online system allows taxpayers to declare and pay their taxes online and make any inquiries. The MoF has two payment gateways: (1) through financial institutions, such as banks, and (2) directly through the MoF portal. According to MoF, over 240,000 taxpayers are registered in the system.

The TIN and associated taxation systems record considerable information about individuals, and they could become a significant authoritative source of trusted data in other digital transactions. Introducing APIs and checking services that allow other services to verify an individual's TIN could be considered in any strategic architecture.

The uniqueness of the TIN could be reinforced by cross-checking the TIN database against a unique ID system – such as the NID database for natural persons, or the commercial registry for legal persons – through an appropriate checking service provided by the relevant entities.

Improving tax collection mechanisms and the uniqueness of the identities of individual and corporate taxpayers would reduce tax evasion, increase government revenues, and broaden the fiscal space more efficiently.

Passports

Lebanese passports are managed by the Directorate of General Security at the MoIM. The passport system is not connected with the NID system, though a NID card is needed to apply for a passport. There is currently no interoperability between the NID card database and the passport database, even though both are managed in-house at the MoIM. This means that direct access to verify the NID is not available during passport application. Thus, there is no way to reliably correlate a passport document number with the unique NID number of the individual passport holder. As with the tax ID and commercial registry cases above, such correlation could be accomplished by MoIM making available an appropriate checking serving allowing NID cards to be validated and the identity attributes they contain to be verified against the NID database.

The passport renewal process could be streamlined and enhanced with a digital service if access to a verification service were provided for NID cards. Passport data itself could also be made available to other services to increase access to services for beneficiaries, such as through ESSN. API access was provided under an ESSN pilot, but it was not utilized and has subsequently been closed. Understanding why this verification was not successful will be important to any subsequent digital transformation project.

Civil Registry

The civil registry is not fully digitized, and the digital civil status records that exist are not interoperable with the NID card database, even though both are managed by the same department (Civil Status) at MoIM. This lack of interoperability prevents the verification of identity attributes, such as name (including spelling, transliteration, and name order) and date of birth on the NID card, against the civil registry, whose birth records are the authoritative source for such data. It also prevents real-time updates between the two systems: for example, name changes recorded in the civil registry during marriage are not carried over automatically to the NID card database, leading to discrepancies. The same is true for other data updates or corrections.

As with the use cases discussed above, a checking service that allows the verification of civil status and NID data is critical. Such checking service would allow civil status records to be robustly linked to NID records in the first instance. In addition, trusted data sharing between the NID and civil registries should be implemented to allow updated data reported to one system to be automatically pushed to the other as a means of keeping both up to date.

Electoral lists

The Lebanese electorate continues to expand, as many expatriates become eligible voters. Furthermore, some voters may have NID cards that are decades old (with correspondingly outdated photos), increasing the risk of misidentification at polling stations. Digitally verifying identity could potentially play a role in limiting misidentification and accommodating the expanding Lebanese voter population, in particular diaspora voters and others who might wish to cast their votes remotely.

For example, uniquely identifying voters by cross-checking electoral lists against the NID system through an appropriate checking service could help ensure trust that each person is only able to vote once. Checking services could also facilitate other routine checks needed to determine voter eligibility, such as verifying if they are in the military or have other disqualifying criteria, and they could also facilitate verification of the appropriate polling station. Additionally, deploying strong digital authentication could support an eventual option to vote remotely (as seen in Estonia, for example) rather than in-person. This could provide certain segments of the electorate, such as citizens living overseas, the opportunity to vote online without the need for costly travel to a physical polling station, which may be a significant distance from their place of residence.

Address database

Lebanon lacks a single authoritative source for residential address data. Address data gathered for the purpose of NID card registration is often outdated, as authorities face difficulties in updating address information, and there is a lack of incentives to keep address data updated. Consequently, many Lebanese citizens' address records remain outdated, even though citizens and residents use governmental services on a regular basis, and often share address data. However, the lack of interoperability and data sharing between governmental systems prevents the updated data from making its way back to MoIM.

As part of digital transformation, there is an opportunity to enable the capture of address data updates as a by-product of digital interactions with governmental services. Such interactions could populate either a single authoritative source for residential address data (against NID number) or provide updates to other ministries as a notification of a change of address.

A key enabling factor of any such service would be the ability to interoperate across government ministries and services. Building such trusted data sharing links with the various governmental (and potentially also private) entities that collect address data as part of their interactions with citizens would allow such updates to be pushed automatically to the authoritative source. This authoritative source of address data could also be queried by those same public and private entities when needing to verify an existing address and ensure consistency across systems, for example by deploying an appropriate address checking service.

Other authoritative data sources

Other functional IDs and registries could be considered as additional authoritative sources of data about individuals. If appropriately digitalized and connected to secure data sharing infrastructure, they could be used for eligibility checking or as part of additional identity verification steps. These additional authoritative sources would be relevant when data is required beyond the basic set of foundational identity attributes managed by the civil registry and NID systems. Such systems could be especially relevant in circumstances where a person needing identity verification is not a Lebanese citizen. Such sources include:

- **Foreigner's database/residency card** – DGCS has a "unique" register/card for foreigners who are legal residents.
- **Refugee database/card** – as managed by the DGCS.
- **Driver's license** – managed by the Traffic, Trucks and Vehicles Management Authority at the MoIM. This system also collects biometrics.

Summary of Digital ID requirements

This section outlines how digital ID could respond to the identification needs of the various sectors described in the previous section, and specifies which digital ID functionalities would be required to enable each sectoral use case. Although some of the functionalities discussed below have applications beyond digital identity, this discussion is limited to their use for a core set of foundational personal data – such as name, place, and date of birth – referred to as identity attributes.

Table 2 maps the core digital identity functionalities (unique identification, checking services, trusted data sharing and digital credentials, digital authentication, and electronic signature) that would be needed to fulfill the various sectoral needs (use cases) identified in the previous section. For each sectoral use case, an indicative level of trust or assurance needed to enable the transaction is also given in the rightmost column; in general, high-risk transactions or initiatives require correspondingly high levels of trust.

Table 2: Summary of Digital ID Requirements for Sectoral Use Cases

Sector	Use case	Main challenges of sectoral initiative	Digital identity functionalities					
			Unique Identification	Checking Service	Data Sharing / Credentials	Digital Authentication	Electronic Signature	Level of Trust[19] (H/M/L)
Financial	Remote Onboarding (eKYC)	Customer due diligence requires robust identity checks during the onboarding of new customers and opening of new accounts for existing customers. Additionally, other attributes required by regulators for AML/CFT reasons, such as residential address, must be collected for clients.		Y	Optional	Y	Optional	M / L
Financial	Credit registry	There is no reliable way to uniquely identify individual credit histories, leading to errors in determining creditworthiness and compromising financial institutions' trust in the credit registry.	Y	Y				M
Financial	Access to Frozen Deposits Deposit insurance	Since there is no unique personal identifier associated with bank accounts, there is no way to reliably associate an individual's financial accounts, both across and within financial institutions. A future deposit insurance scheme based on a per-person (as opposed to per-account) payout ceiling will be highly vulnerable to fraud unless account holders can be uniquely identified. Partial access to frozen deposits under the BDL's Circular 158 is capped on a per-individual basis, requiring bank accounts to be uniquely identified to confirm eligibility.	Y	Y				H
Social protection	Social assistance (targeting)	It is impossible to verify eligibility for social payments by verifying data produced or managed by other sectors or ministries. Data on key determinants of eligibility – such as income, tax, eligibility for subsidies, or household composition – is unavailable, reducing the ability to efficiently target social assistance. Vulnerabilities include the ability to falsify self-declared eligibility data, necessitating a costly additional in-person verification.			Y			M

19 The required level of trust, or assurance, is estimated as high (H), medium (M), or low (L). This rating is based on the approximate risk level of the underlying transaction: transactions that expose sensitive personal data or have a high financial value are typically considered high-risk. The estimated level of trust required should be considered as indicative.

Sector	Use case	Main challenges of sectoral initiative	Digital identity functionalities					
			Unique Identification	Checking Service	Data Sharing / Credentials	Digital Authentication	Electronic Signature	Level of Trust[19] (H/M/L)
Social protection	Social assistance (registration)	The ESSN beneficiary database was based on an online registration process without a trusted identity verification process or trusted unique ID in place, opening the potential for fraudulent and duplicate registrations. Vulnerabilities include multiple registrations by an individual and double counting of household members.	Y	Y		Optional		M
Health	Medical records (data sharing)	Health centers are unable to share data on treatment, resulting in incomplete medical records, duplicate care, and treatment decisions made based on incomplete information.	Y		Y			H
Health	Medical records (creation)	The in-person onboarding required during the creation of a medical record requires the patient to have her medical record created as an additional step before treatment, or else receive treatment at a medical center that also offers an onboarding service.	Y	Y		Optional		H
Health	Medical records (access)	Patients do not have access to their medical records. Making such information available based on current systems would be an unacceptable privacy risk, as it is not possible to securely manage access to the health records.			Optional	Y		H
Health	Visa process Medical insurance claims	The process for verifying the eligibility of medical claims for reimbursement is paper-based, in particular medical visas. This leads to inefficiencies and is a barrier to moving insurance reimbursement online.	Y				Optional	H
Health	Remote medical consultations	Doctors are unable to verify the identity of patients during a remote consultation, and key process elements such as gaining access to a patient's medical record, cannot be done remotely.			Y	Y		H
Health	Tracking medications	The MediTrack system has been created to track prescriptions and payments for medicines. Yet the system lacks a unique identifier for patients across all medical systems, making it difficult to create a single, encompassing view of patient records, and complicating the effort to reduce the incidence of duplicates.	Y			Y		H

Sector	Use case	Main challenges of sectoral initiative	Digital identity functionalities					
			Unique Identification	Checking Service	Data Sharing / Credentials	Digital Authentication	Electronic Signature	Level of Trust[19] (H/M/L)
Commercial	Real estate	There is no link between the NID number and land registration, although NID cards are widely adopted and the land registration database includes a data field for the NID number. A previous analysis of 100,000 land ownership records against the NID card database could only confirm the property owners' identity in approx. two-thirds of cases.	Y	Y		Y	Y	H
Commercial	Commercial register	The commercial register requires the in-person presentation of NID cards or passports of the company's responsible officers. Verification of these key documents is manual and time-consuming for both the responsible officers and the government officials performing verification. Lack of digital validation and verification leaves the commercial registry vulnerable to fraud based on multiple registrations and association with fictitious directors.	Y	Y		Y		M
Public administration	Civil servants' registry	Utilizing the NID number as the primary identifier in the Civil Servants' Registry can reduce administrative overhead, duplicate wage payments, improve integration to tax systems, and make it simpler for civil servants to change jobs and start new positions.	Y	Y				M
Public administration	Tax	There is inadequate assurance of the uniqueness of the TIN due to the lack of ID verification of physical persons (against the NID) and legal persons (against the commercial registry).	Y	Y				M
Public Administration	Civil status records	The civil registry is not fully digitized, and the existing digital civil status records are not interoperable with the NID card database. This prevents the verification of identity attributes, such as name (including spelling and name order) and date of birth on the NID card, against this authoritative source.	Y	Y	Y			M

Sector	Use case	Main challenges of sectoral initiative	Digital identity functionalities					
			Unique Identification	Checking Service	Data Sharing / Credentials	Digital Authentication	Electronic Signature	Level of Trust[19] (H/M/L)
Public Administration	Biometric passports	The NID card is often used for verification of identity and eligibility for a passport application. There is no interoperability between the NID card database and other services, meaning that access to a verification service provided by the NID card system is not available.	Y	Y				M
Public Administration	Address database	Lebanon lacks a single authoritative source for residential address data. Address data gathered for the purpose of NID card registration is often outdated as authorities face difficulties in updating address information. Consequently, many Lebanese citizens' address records remain outdated, even though citizens and residents use governmental services on a regular basis, and often share address data.		Optional	Y			M
Public Administration	Electoral lists	The Lebanese electorate continues to expand as many expatriates become eligible voters. In addition, there are concerns regarding voter fraud and misidentification at polling stations. Digitally verifying identity could play a significant role in preventing voter fraud, limiting misidentification, and accommodating the increasing Lebanese voter population.	Y	Y		Y		H

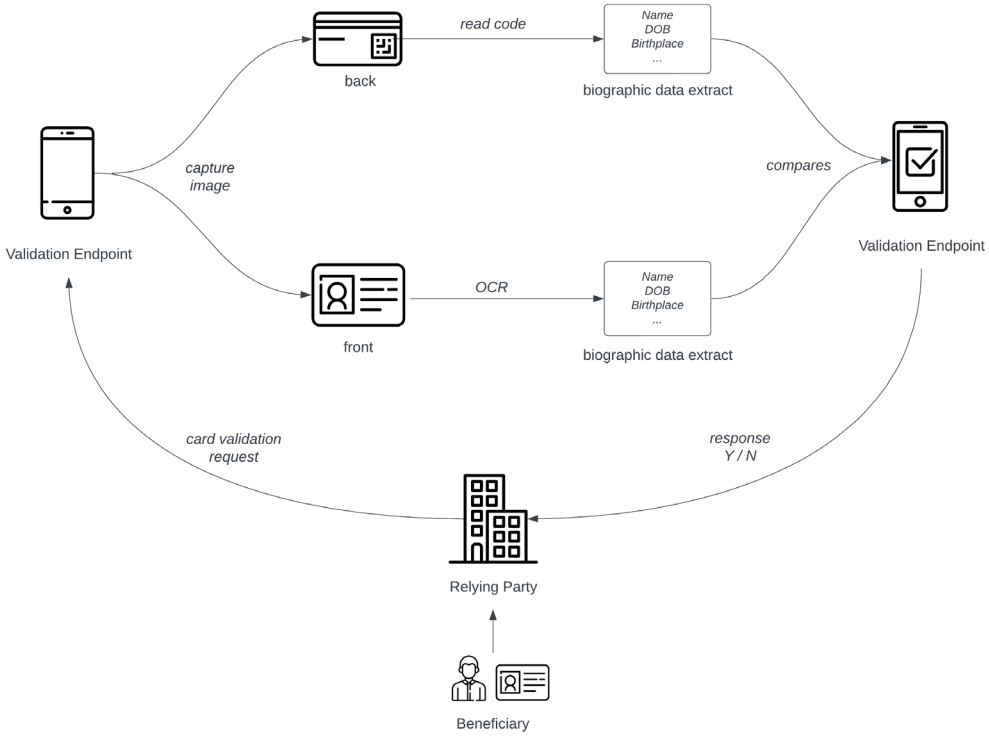
Recommendations

The recommendations below are based on an analysis of the potential benefit of implementing digital identity functionalities into existing systems and practices within Lebanon, and could be evaluated for potential incorporation as the Lebanese government considers the implementation of digital ID systems.

Quick Wins

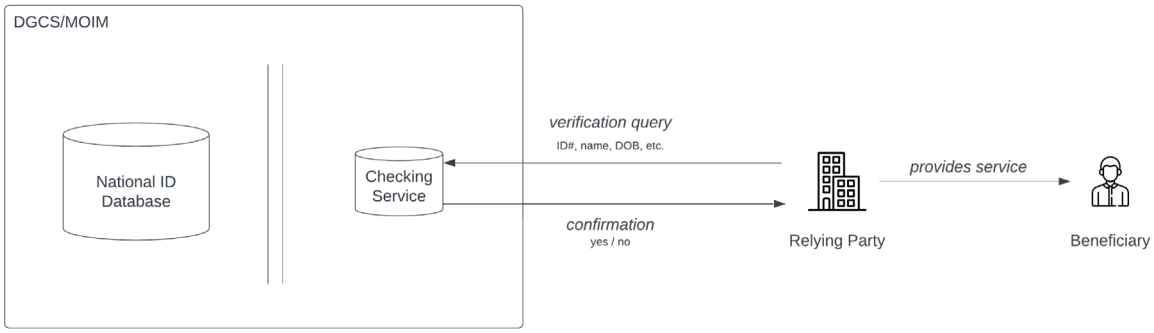
Enable service providers to validate NID card using the existing bar code. Since the NID number is currently readable in plaintext in the barcode, the MoIM could provide a solution to relying parties that allows the authenticity of a NID card, including its biographic data, to be verified digitally. This would greatly enhance trust in the validity of the NID card by addressing a commonly held stakeholder perception that a multitude of NID cards in circulation are fraudulent. Figure 4 illustrates an indicative ID card validation workflow using the barcode on the existing NID card and a software application made available by MoIM.

Figure 4: Indicative ID Card Validation Workflow



Implement checking services to verify data from core authoritative sources. Enabling services across government to check the validity of official documents or identifiers against the authoritative source (e.g., NID card) will enable remote onboarding for digital services that would have previously required in-person document checking. Creating secure checking services could be explored as a building block of a high-trust digital economy. If implemented according to good practice models, such checking services would not need to share personal data with service providers, nor would they need to connect backend production systems to the internet or otherwise expose them to cyberattacks. An illustrative example of how a checking service can support service delivery is provided in Figure 5 (an indicative security architecture can be found in Annex 3).

Figure 5: Illustrative Example of an Identity Attribute Checking Service



Leveraging the NID for unique identification. Using a single identifier for individuals reduces the need for identity matching and makes it easier for governmental services to interoperate. Attributing the NID to user accounts in core services (e.g., health) by first verifying the person's identity to a high level of certainty will increase trust when transacting across government. While a 2017 decree mandates the UIN of the NID system to be used as the sole personal identifier across governmental systems, this has not been implemented, and requires additional policy guidance as well as sufficient digital safeguards to be in place, notably for cybersecurity and data protection.

Short Term

Conduct civil society consultations and end-user research to inform broader digital ID strategy. While the present analysis has focused on the limitations of current systems and the digital ID needs of various sectors, further work is needed to clarify citizens' needs, pain points, and concerns related to digital systems. This may generate additional recommendations and requirements for a future digital ID, as well as begin to create buy-in and trust for such a solution. Consultations should be broad and capture the needs of all in society, including marginalized and vulnerable groups (such as foreign populations and refugees).

Establish interoperability between NID card and passport databases. One of the main motivations for implementing sectoral unique identifiers is that the various MoIM-issued identity credentials do not fulfill this purpose. While, in theory, the NID number could play this role, such capacity is undermined by a lack of linkage to the passport database: if a person registers for a service using a passport, there is no way to verify that same person is already registered under a NID number. A checking service implemented at MoIM that allows the correlation of passport document numbers (which change with each passport issued) to the person's corresponding NID, could resolve this issue and increase uptake of the NID number as a unique identifier by service providers.

Identify authoritative sources of data. There are multiple data sources across governmental ministries and agencies that provide the backbone of current service delivery. Some of these sources, along with their associated credentials, form the basis of identity and eligibility in Lebanon today. Examples include ID cards, passports, driving licenses, tax identification numbers, and health IDs. Rapid analysis could be conducted to determine where these authoritative datasets are used indirectly in service delivery, and where they could be used further to reduce red tape, increase inclusion, and reduce costs to government and/or citizens. A clear designation of authoritative sources will address several concerns with the current ID ecosystem, including: (a) the proliferation of outdated data in official databases, including the NID card system, and a lack of incentives for individuals to update authoritative sources; (b) discrepancies in identity attributes and other data across governmental systems caused by a lack of mechanisms to facilitate data updating; and (c) the lack of a method to adjudicate which version of a person's data should be retained for official use when there is a discrepancy between data sources.

Develop data governance and data classification policy. If data sharing becomes more widely adopted, as industry best practice suggests, then underlying data governance will become ever more important, as will the ability to classify data based on its use and sensitivity using standardized measures. Drafting appropriate policies early in the implementation cycle is vital, as they will be instrumental in shaping any eventual architecture and service design.

Medium Term

Strengthen legal and institutional enablers for digital ID, including cybersecurity and data protection. The existing legal framework that governs digital ID in Lebanon requires comprehensive updates to facilitate the digitalization of both ID and CR systems, ensuring the protection of personal data and the security of these systems. The implementation of regulations is necessary to fully operationalize the adoption of the NID, following the 2017 decree,[20] along with establishing protocols or memoranda of understanding between DGCS and relevant authorities utilizing the NID database. Furthermore, amendments to the 1951 civil registration law[21] are essential to streamline current paper-based processes, especially for the registration of vital events such as births, to accommodate digitalization. The legal recognition of digitalized identity documents currently hinges on the adoption of the e-signature implementing regulation submitted to the Council of Ministers in January 2024. Collaboration among pertinent authorities is also crucial for a unified framework for e-signatures across sectors. Lastly, to ensure robust safeguards for the digital ID system, enacting a comprehensive data protection law is vital, addressing gaps in Law 81-2018[22] and establishing an independent oversight agency, currently absent from the national landscape. Periodic reviews and updates of cybersecurity measures are necessary, and the adoption of comprehensive cybercrime legislation, particularly incorporating provisions on international cooperation, is encouraged, to align the Lebanese cybercrime framework with international instruments such as the Budapest Convention.[23]

---

20 Decree 168 issued on February 23, 2017, establishing rules and procedures for the adoption of the unique identification number of citizens for public administrations, public institutions, municipalities, and other public authorities.
21 Law on documenting personal status, issued on December 7, 1951.
22 Law No. 81 of 10 October 2018 on Electronic Transactions and Personal Data.
23 Convention on Cybercrime (ETS No. 185) of November 23, 2001.

Improve the existing NID card provision as part of wider digital transformation. The current NID card, first introduced in 1997, is notably limited in its ability to verify identity. Implementing digital identity will not remove the need for a NID card, as digital identity is reliant on the verification and issuance processes of the NID card and the data it gathers. In this respect, any changes to NID card specifications should consider a complementary relationship with digital identity moving forward. As part of the rollout of the next-generation NID card, attention should be given to supporting systems to improve their robustness and resilience, including updating the card's design. As part of the transition, a comprehensive cleaning exercise could be undertaken to recollect data that is of poor quality or out of date, such as childhood facial photos, or legacy fingerprint biometrics that were originally collected using ink and paper. The new system could also include mechanisms in place to ensure that data is kept up to date, through a combination of interoperability with other data sources and appropriate incentives for individuals.

Develop multiple alternatives for digital identity to meet the needs of various user categories. Digital identity should not intend to replace existing identity means (e.g., NID cards and passports), but make it easier and safer for individuals to perform both online and offline transactions by extending the reach of existing proof of identity to online services and in-person transactions. Such transactions can be performed without oversharing data or requiring individuals to carry around multiple high-trust documents. Digital identity, for example, offers the ability to challenge individuals to authenticate themselves by confirming that they are not just in possession of appropriate credentials, but by also proving that they are the actual persons to which these credentials were issued. The opportunity to issue a digital identity credential could be considered in cases where high-trust credentials are currently issued (e.g., ID cards and passports). Such an opportunity is favorable given the strength of existing identification processes and the security of the issuance process. This is also an ideal opportunity for individuals who wish to receive a digital credential (e.g., a mobile ID). MoIM could consider piloting digital identity functionality, such as a digital identity smartphone application for citizens with access to mobile devices, as an additional modality that complements the existing or future NID card. The design of multiple digital identity credentials to meet the needs of various user categories should be informed by a broader digital ID strategy and consultations with civil society, including marginalized and vulnerable groups. Feasibility studies and cost-benefit analyses should be conducted to analyze alternative delivery models for digital ID and inform a roadmap for implementation.

Increase trusted data sharing and user-centric control. Alongside the continued identification of authoritative data sources in government, further efforts to create a wider, trusted data sharing architecture could be considered. Activities could include the legal, business, and operational elements of creating a wider trust framework that will be reflected in policies, guidance, and perhaps additional legislative changes to allow more government ministries and their services to accept trusted data from digital sources.

Provide support to relying parties for wider rollout of digital identity. Service providers who rely on digital identity verification, known as relying parties, will be focused on their primary activities and policies. Relying parties may find that although digital identity and trusted data sharing are advantageous from an efficiency perspective, such technical advancements may be difficult to implement within existing capacity if adoption overhead is too great. Providing support to relying parties, ranging from guidance and training to implementation support and example code, will be important to lower the barriers to digital identity adoption. A technical engagement team could be created to work closely with high-impact relying parties to ensure they are guided through onboarding.

Long Term/Strategic

Achieve legal equivalence of digital identity and electronic signatures. Electronic signatures already enjoy legal equivalence with wet signatures in Lebanon through Law 81-2018, but the latter is not yet implemented due to a lack of an appropriate regulatory framework. Implementing electronic signature legislation based on a robust digital ID system is a prerequisite for scaling the digital economy by extending trust to higher-value transactions. The ability to robustly prove one's identity and transact securely online is especially relevant to Lebanon due to its large diaspora population.

Develop data sharing architecture for the whole of government. In addition to identifying and utilizing authoritative datasets across government, consideration should also be given to how governmental services are architected. The existence of duplication causes certain types of data (e.g., address data, contact details, and organizational datasets) to be outdated and unsynchronized. Authentication to services may utilize differing registration processes and credentials, which could be reduced through the federation or reuse of those credentials. Efficiencies could also be realized in service delivery and development, enabling access to eligibility data from multiple governmental data sources. All these needs could be factored into future architectures for governmental IT systems, including the growing use of digital as a means of access for citizens and civil servants.

Enable citizens to manage their own data. Individual citizens are uniquely positioned to know when their personal data changes or where errors exist in governmental records. For example, citizens know immediately when changes occur to their residential address (and/or correspondence address), yet significant time could pass before the relevant ministries are notified. This is largely because each ministry maintains its own records for citizens, and citizens are often only compelled to notify those ministries when they need services. This can lead to mismatches in governmental datasets, and consequently impact both service delivery and planning. Error in governmental records can be reduced by enabling citizens to authenticate themselves using digital identity, and by allowing them to manage their personal data. Citizen-performed updates can be sent automatically to all ministries, thereby simplifying user interaction with government and ensuring data is accurate and up to date. Long-term strategic plans could consider such services and how the citizen can play a more immersive role in their own service delivery.

Implement a national population registry to complement existing systems. Existing sources of foundational ID data in Lebanon exist for specific purposes, such as issuing national ID cards or managing birth records. Consequently, eligibility criteria for these systems are limited (for example, to citizens or to persons born in Lebanon). Implementing a population registry to help underpin these existing systems and integrating limited additional foundational data (e.g., residency status) could help improve identification, provision of public services, statistical analysis, and policy planning. MoIM could implement such national population register as an interoperable complement to its existing systems.

Technical Annex

This technical annex provides indicative implementation details for selected quick wins highlighted in the report, along with some effort estimations for their initial development and limited-scale deployment.

Annex 1: Implementation Requirements (Quick Wins)

The following modules could be deployed in the short term to extend existing systems, with minimal investments, to improve the relevance of the NID system to service providers through support for key digital identity use cases. These implementation requirements concern only those recommendations identified as "quick wins" in the above analysis.

1. **Barcode reader application.** The development of a smartphone app that can read the 2D barcode is relatively feasible based on widely available tools and software libraries. Optionally, this app could include user biometric authentication by matching facial biometric data with the photo displayed on the NID card, where this data is available (QR code, MoIM service, or scanned document image). There are multiple providers and tools available to provide this capability.

2. **Document validity checking service.** A main concern of service providers is that they have no way to check that the attributes written on the NID card are valid. A checking service could be implemented to, for example, compare the scanned image of the NID card (via OCR) with the reference data on the barcode and/or MoIM servers. Such a checking service could implement secure open standards (e.g., based on OpenID Connect) to facilitate data retrieval from a server, or be carried out in a decentralized manner (e.g., using the barcode). To ensure privacy and security, these services would be created separately to operational systems and physically and technically secured on separate network segments.

3. **Trusted identity attribute sharing using barcode.** A service for the verification of the barcode and selective retrieval of data (e.g., birth date and place of birth) could be developed and made available to authorized service providers to ease data entry burdens and reduce errors.

In addition to developing new software modules to facilitate NID card validation and data sharing, the following non-technology quick wins would promote adoption and trust in these new digital ID services:

4. **Publishing a policy on unique identifiers.** Having a single identifier for individuals reduces the need for identity matching and makes it easier for governmental services to interoperate. Appropriate policy and guidance are needed for how this should be achieved.

5. **Onboarding of first digital service.** Appropriate personnel should work with the service developer to support and provide guidance during the integration of verification of data and use of checking services (as applicable). Social protection could be a candidate service, although there is also significant demand from other sectors, including health and banking.

6. **Identification of authoritative data sources.** As a first step toward the development of a broader data governance framework, this quick win would entail consulting with stakeholders for the identification of authoritative sources to meet eligibility requirements of digital services.

The implementation requirements, along with an indicative estimate of the effort required for implementation, are summarized in the tables within this technical annex.

These indicative estimates are to implement a limited-scale version of the above systems to support one or two pilot applications. Scaling these systems – to improve availability and to support real-time transactions across multiple sectors with a defined service-level agreement – would require additional investment, particularly to the underlying hardware and hosting capacity.

Annex 2: National ID Card Validation Service

Enabling service providers to validate NID card using the existing barcode

Since the NID number is currently readable in plaintext in the barcode, the MoIM could provide a solution to relying parties that allows the authenticity of a NID card, including its biographic data, to be verified. This would greatly enhance trust in the validity of the NID card by addressing a commonly held stakeholder perception that a multitude of NID cards in circulation are fraudulent.

The resulting app would be developed for iOS and Android, and would allow a user to scan an ID card to OCR data printed on the card surface; this data would then be compared to a reading of the 2D barcode from the same card. The resulting verification against the 2D barcode will provide the relying party with a level of certainty that the card itself is genuine, although card validation against the authoritative source will not have occurred. The validity check could be added in the future if the checking service (against MoIM's ID card data) could also be made available.

Indicative app development effort

	Task	Estimated time to complete
1	Inception	2 weeks
2	App UX design and user testing	3 weeks (concurrent with task 3)
3	App build sprints (5 x 1-week sprints)	5 weeks
4	Private beta app testing	2 weeks
5	Deployment to app store / final go-live provisioning	1 week
	TOTAL	**10 weeks**

Annex 3: Identity Attribute Checking Service

Implement checking services to verify data from core authoritative sources

Enabling services across government to check the validity of official documents or identifiers against the authoritative source (e.g., NID card) will enable remote onboarding for digital services that previously would have required in-person document checking. Creating secure checking services could be explored as a building block of a high-trust digital economy. If implemented according to good practice models, such checking services would not need to share personal data with service providers, nor would they need to connect backend production systems to the internet or otherwise expose them to cyberattacks.

The proposed service

The proposed service is a checking service that enables a trusted institutional relying party, such as the Ministry of Social Affairs (MOSA) or the Presidency of the Council of Ministers (PCM) in the case of ESSN, to check that the NID card number submitted for authorization or eligibility purposes by a beneficiary is valid and correct for the person applying.

To achieve this, a checking service based on a secure API Gateway approach is proposed that:

- Fully protects MoIM systems.
- Does not share or disclose any personal data.
- Renders the checking service accessible only to registered institutions such as MoSA.
- Implements multiple layers of security.
- Ensures that all access to the checking service is monitored and auditable.
- Removes the need for direct integration with existing MoIM systems.
- Does not require 24x7 availability or access to MoIM systems.
- Does not require modification to existing MoIM systems.

Data payloads and responses

Data disclosure would be minimized where appropriate and only response codes (e.g., valid/invalid) and not actual MoIM data would be returned in responses. All data would be cryptographically signed and encrypted to ensure integrity and confidentiality.

Request payloads (indicative):	
National ID number	As asserted by the applicant / relying party service
Family name	As asserted by the applicant / relying party service
Date of birth	As asserted by the applicant / relying party service
Match status	• Valid (V) • Invalid (I) • Not Found (N) • Service Unavailable (U)

MoIM data never leaves MoIM

The proposed service is a checking service; therefore, no data would be shared outside of MoIM. Only the result of a 'check' against the ID card database would be extracted. As the system configuration would not allow any data other than the predefined set of response codes to be emitted through the API, the risk of breaches of sensitive MoIM identity data would be minimized.

The matching process itself would also occur inside MoIM's infrastructure by a service that is isolated from internet access.

Minimum impact on the existing Idemia solution

No modifications would be required to the underlying Idemia identity system. The only requirement would be to export a subset of the NID card database to be referenced by the ID card checking service. This subset could exclude any data fields that are not relevant to the checking service or that are considered sensitive, such as religion or biometrics. This export could be as simple as a flat file (e.g., CSV).

Availability of MoIM services is not critical

Relying party services (e.g., ESSN) wishing to check a NID number would do so by calling an API served by the API gateway and would never directly access MoIM systems. Equally, access to the production ID card system database would not be required to service API calls, as a separately hosted subset of the data, a checking database, is used by the ID verifier service. The ID verifier service itself does not need 24x7 availability as uniaxiality can be flagged by the outward-facing API gateway endpoint, alerting the relying party to the status of the service. The relying party would then make a risk-based decision on the result of a call to the checking service, as the result may be Y/N or Unavailable.

Individual zones are secured from each other and the internet

Beyond the internet-facing API endpoint for relying parties, all processing of API requests and MoIM data (when validated) would be undertaken in separate zones that are isolated from the internet and other services. Traffic from each zone would be restricted by validating proxies and routers to prevent abnormal flow of data. Each of these zones may be monitored separately, hosted separately, and have services that are cycled regularly to prevent potential compromise. An indicative security architecture can be found in Figure 6 below.

The integrity and confidentiality of all data, requests, and responses is protected

Requests and responses passed from service to service (including the initial API call from the relying party) would be signed and encrypted using the public/private key technology. Private keys would be confirmed during relying party verification and access to public keys provided on restricted lists. Key pairs for transactions between Zone 1/2/3 services would never be shared with the relying party as they are for internal processing.

All data at rest and in transit would be signed and encrypted including the API request (from the relying party) and the ID card checking database (even though this is internal to MoIM and is never accessed directly).

Indicative high-level architecture

Process flow steps (all systems available):

Step 1 – Relying party registers with the API gateway service. This requires the relying party to complete an offline application process that is controlled by services operator and MoIM.

Step 2 – Registered and verified relying party is initiated with private keys for access to API services. Access keys and security credentials are exchanged out of band (i.e., not over the internet or email).

Step 3 – Onboarded relying party requests national ID check using the appropriate API gateway endpoint.

Step 4 – The API request is verified and validated, then the validating proxy service calls the appropriate API endpoint in non-web-facing Zone 1. Access to Zone 1 is via a HTTP protocol enforcing reverse proxy.

Step 5 – The request, if still valid, is passed via a separate validating proxy to an ID card agent in a separate network zone (Zone 2).

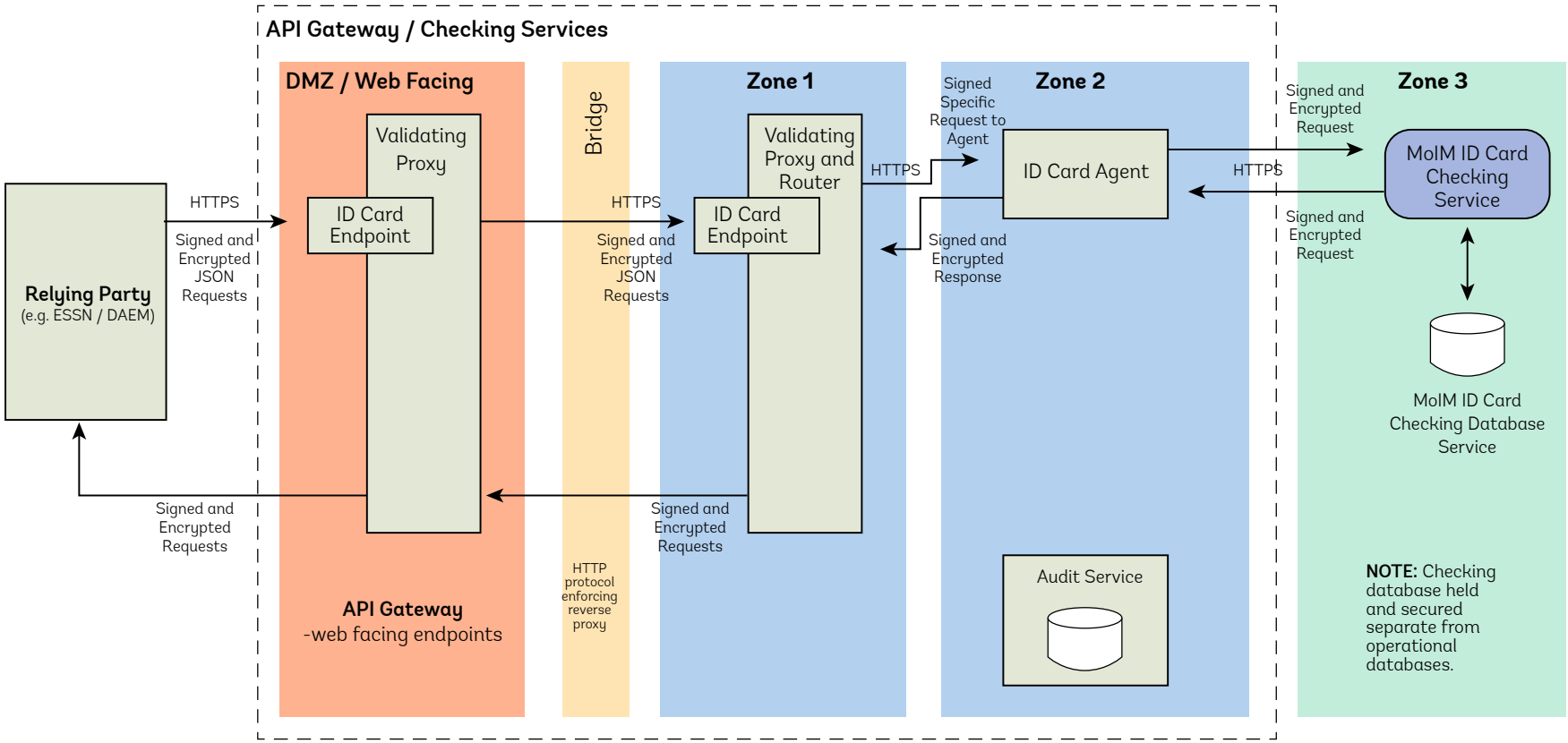
Step 6 – The request is finally passed to the MoIM ID card checking service (Zone 3 internal to MoIM) and the matching query is executed.

Step 7 – The result of matching is passed back through the respective calling services to the API gateway and on to the calling relying party for reference.

Indicative Development Effort

	Task	Estimated time to complete
1	Inception	2 weeks
2	Definition of architecture and service design	4 weeks
3	Implementation and configuration of security zones and servers	3 weeks (concurrent with task 4)
4	Development of API gateway and intermediate services (4 x 2-week sprints)	8 weeks
5	Private beta testing with a single service (restricted access)	3 weeks
6	Final go-live provisioning	1 week
	TOTAL	**18 weeks**

Figure 6: Indicative Security Architecture for an Identity Attribute Checking Service



Source: World Bank

Note – If any of the services from Zone 1 to 3 are offline/unavailable when called, an error code will be returned to the API gateway, which will notify the relying party that the service was unavailable.

Annex 4: Unique Identifier Policy

Produce policy and/or guidance that accepts NID as the unique identifier for citizens

Having a single identifier for individuals reduces the need for identity matching and makes it easier for governmental services to interoperate. Attributing the NID to user accounts in core services (e.g., health) by first verifying the person's identity to a high level of certainty will increase trust when transacting across government. Producing policy and/or guidance for how this could be achieved and maintained should be considered.

Indicative policy / guidance development effort

	Task	Estimated time to complete
1	Inception	2 weeks
2	Definition of document outlines for 1 policy and 1 guidance document	1 week
3	Drafting of 1 policy and 1 guidance document	3 weeks
4	Review and amendment process	2 weeks
	TOTAL	**8 weeks**


THE WORLD BANK
ID4D
IDENTIFICATION FOR DEVELOPMENT