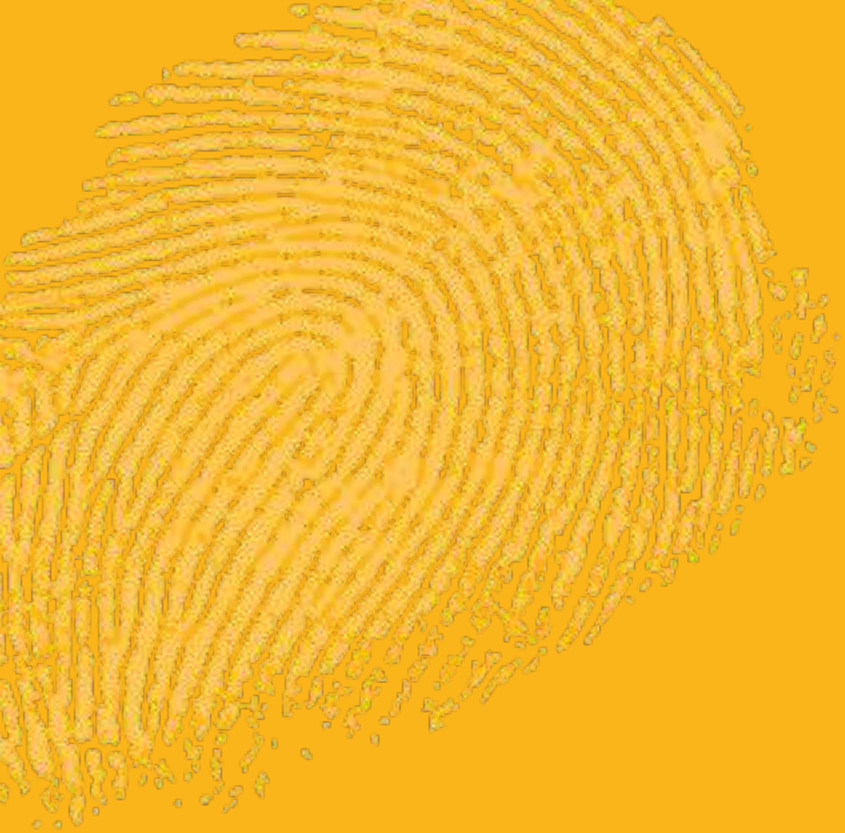


Building trust in ID systems

James Neumann, Senior Counsel

THE WORLD BANK

Contents

Digital ID as a priority

Privacy and data protection

Inclusion

Design

IDEEA Guidance Note

Core needs for digital ID systems

The Identification Gap

SDG Target 16.9: By 2030, **provide legal identity for all**, including birth registration

Globally, an estimated
1.1 billion people
are unable to prove their identity

Many **refugees and IDPs lack legal identification**: ID documents are often lost, destroyed, or confiscated or may have never been issued

The Authentication Gap

Even with ID, it may be impossible to **verify validity** + **authenticate holder** against claimed identity

Credentials that cannot be verified will only provide **a limited level of assurance**, and may not be widely accepted

Exclusion

Cross borders safely and legally

Prove eligibility for and access social and health benefits

Access financial services, mitigate ID theft, AML/CFT compliance

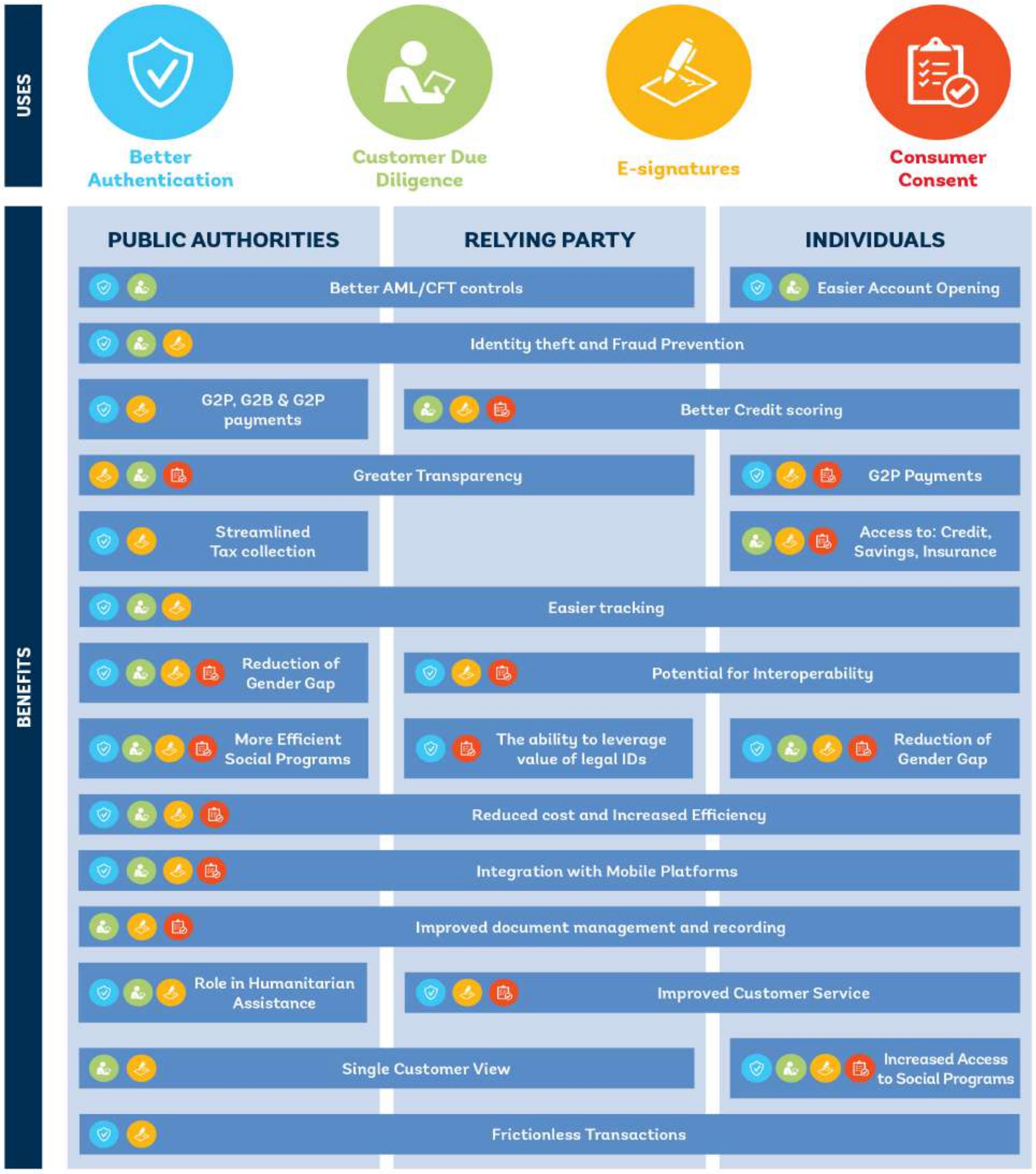
To participate in the (formal) economy

…

Additional benefits of digital ID

- Digital ID systems can enable and improve numerous **public and private sector services and transactions**

- Digital ID systems **support development goals:**
  - Access to finance
  - Gender equality and empowerment
  - Access to health and education services
  - Child protection
  - Increased migration and labor market opportunities
  - Improved access and quality of social protection
  - Improved governance



USES

Better Authentication

Customer Due Diligence

E-signatures

Consumer Consent

BENEFITS

PUBLIC AUTHORITIES

RELYING PARTY

INDIVIDUALS

Better AML/CFT controls

Easier Account Opening

Identity theft and Fraud Prevention

G2P, G2B & G2P payments

Better Credit scoring

Greater Transparency

G2P Payments

Streamlined Tax collection

Access to: Credit, Savings, Insurance

Easier tracking

Reduction of Gender Gap

Potential for Interoperability

More Efficient Social Programs

The ability to leverage value of legal IDs

Reduction of Gender Gap

Reduced cost and Increased Efficiency

Integration with Mobile Platforms

Improved document management and recording

Role in Humanitarian Assistance

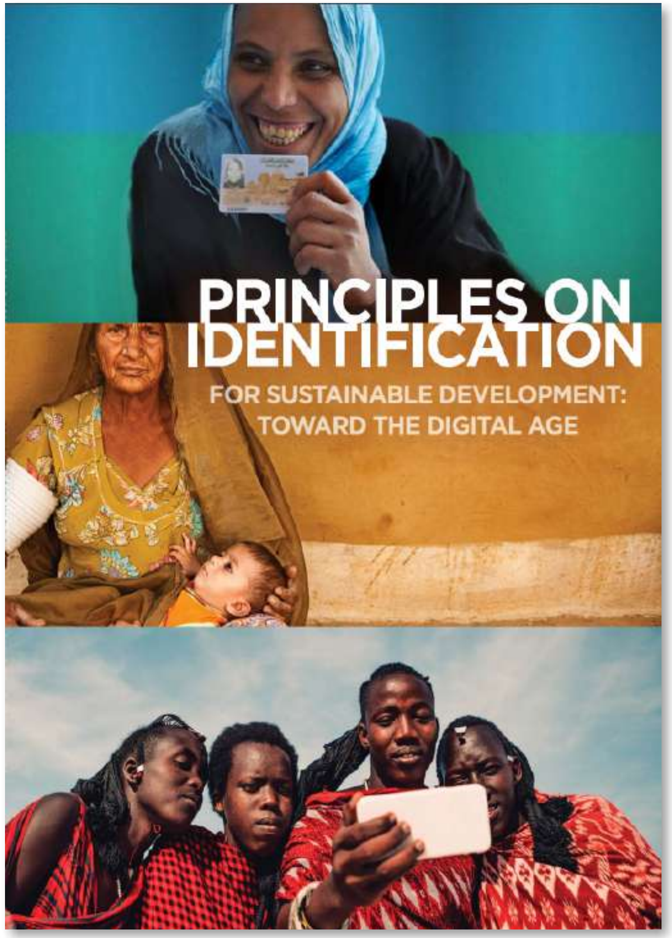
Improved Customer Service

Single Customer View

Increased Access to Social Programs

Frictionless Transactions

Legal and technical design aims to support the 10 Principles on Identification


PRINCIPLES ON IDENTIFICATION
FOR SUSTAINABLE DEVELOPMENT: TOWARD THE DIGITAL AGE

Inclusiveness: Universal Coverage and Accessibility

1. Universal coverage for individuals from birth till death, **free from discrimination**
2. **Barrier free access**, including information, technology disparities, or direct and indirect costs

Design: Robust, Secure, Responsive, and Sustainable

3. Establishes a **robust** – unique, secure, and accurate – identity from **birth till death**
4. Platform is responsive to the needs of users and interoperable
5. **Collects and uses data proportionally and with minimal disclosure**
6. Uses **open standards** and is vendor and technology neutral
7. Financially and operationally **sustainable** without compromises on access

Governance: Trust, Privacy, and User Rights

8. **Comprehensive legal and regulatory framework which safeguards user rights and data privacy & security**
9. Established and clear **institutional mandates** and accountability
10. **Enforced legal and trust frameworks through independent oversight and adjudication of grievances**

Sustainable Development Goals (SDGs)

Goal 16 Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels

16.3 Promote the rule of law at the national and international levels, and ensure equal access to justice for all

16.9 By 2030 provide legal identity for all including free birth registrations

SUSTAINABLE DEVELOPMENT GOALS
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS
SUSTAINABLE DEVELOPMENT GOALS

Contents

Digital ID as a priority

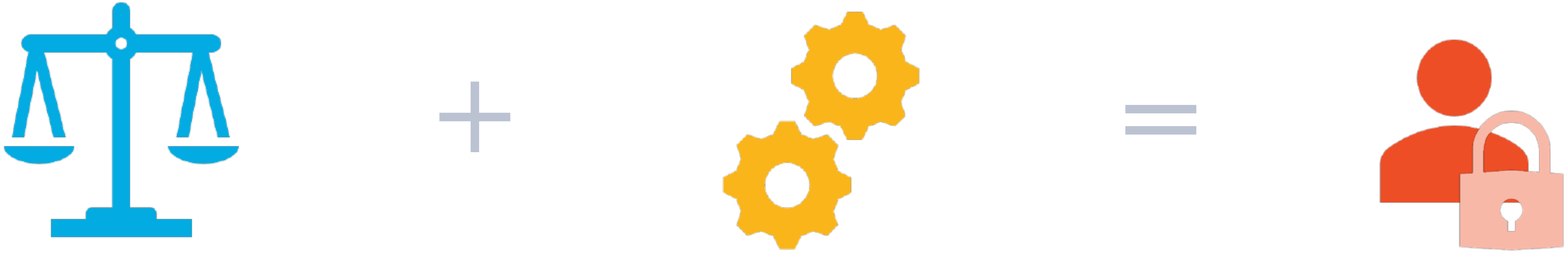
Privacy and data protection

Inclusion

Design

Legal assessment

ID4D opted for a techno-legal approach to enable the design of systems which protect privacy and user rights & control



Legal/Regulatory Trust Framework

E.g. Privacy and data **protection laws**, clear **institutional mandates**, enforcement **authority**

+

Privacy by Design Techniques

E.g. encryption, tamper proof **audit logs**, data **portability**, authentication **alerts**, and access **controls**

=

Robust, Sustainable System

Ensures user **privacy & data protection**, and enables sharing of data only with **consent**

ID Enabling Environment Assessment (IDEEA) ✚ Report on Privacy by Design Techniques ➡ ID4D Approach

Why privacy and data protection is a concern

- ID systems involve capture, storage and use of personal data, so there are inherent **risks of privacy violations, data and identity theft, misuse and discrimination**

- If individuals feel that privacy is not safeguarded, they may **withhold information**, supply **inaccurate information** or simply **avoid participating** (history is littered with failed systems)

- **Third party participants and users of the scheme** need to trust it works effectively and allocates appropriate responsibilities

Elements of a sufficient framework

- Country-specific legal protections for privacy and data protection can be addressed through:
    - **A generally applicable legal framework** or
    - **Specific provisions included in the ID system's legal framework**

- An adequate framework will require:
    - **Data security**: secure storage of data and notification of breaches
    - **Limitations on data collection and use**: only for express purposes, only to the extent and for so long as is necessary, and under a lawful basis (such as consent)
    - **Transparency**: individuals should be informed of which data is collected and how it will be used
    - **Individual privacy rights**: rights to access, review and rectify data, and appropriate mechanisms for complaints and redress (sometimes also to port and delete)
    - **Robust institutions**: capacity and independence to implement and enforce the framework

Contents

Digital ID as a priority

Privacy and data protection

Inclusion

Design

Legal assessment

Inclusion

- An ID systems with **rigid eligibility requirements, high fees or geographic, linguistic or other barriers to registration** may unintentionally exclude certain populations

- An ID system that is not inclusive **risks marginalizing vulnerable populations**

- If an ID system replaces alternative or informal means of proving identities, **excluded populations may be unable to access essential services** or otherwise reap the benefits or participation

Eligibility

- Promoting inclusion requires **minimizing unnecessary eligibility barriers**
- Ideally, **all residents, regardless of citizenship status, should be eligible** for registration, including refugees and stateless individuals (even if systems may collect different information or have alternative credentials depending on citizenship status)
- **Registration of children has benefits but requires careful thought**
    - Registration can facilitate access to public benefits and services and help to prevent child trafficking and child labor and track vaccination and other health history
    - But children are more likely to be the victims of identify theft and are unable to give meaningful consent to data collection
- **Requirements for establishing eligibility should be flexible** to avoid excluding vulnerable populations without birth certificates or other documents

Accessibility

- Another means of promoting inclusion is to **ensure accessibility to registration** in the ID system

- To minimize poverty as a barrier, **registration should be low-cost or free**
  - Each ID system must balance accessibility with financial sustainability

- To minimize geographic isolation as a barrier, **registration facilities should be accessible in remote areas**, facilitated through:
  - Private sector outsourcing to expand the number and reach of registration facilities
  - Mobile registration facilities that travel to remote locations

- To minimize cultural barriers, **registration facilities should have staff fluent in local languages and familiar with local customs**

Non-discrimination

- If individuals feel that an ID system is discriminatory or can be used as a tool for further discrimination, they may **withhold information**, supply **inaccurate information** or simply **avoid participating**

- Country-specific legal protections for non-discrimination can be addressed either through:
  - **A generally applicable legal framework** or
  - **Specific provisions included in the ID system's legal framework**

- To prevent the use of the ID system as a tool for discrimination **sensitive information about individuals (e.g., race, religion, ethnicity)** should:
  - Not be collected, or
  - Not be displayed on a credential, discernible from an ID number, or otherwise accessible to third parties (other than those who require it)

Mandatory vs. voluntary

- While mandates to register may increase inclusion, **voluntary systems are preferred** because they engender trust and preserve liberty

- Two types of mandates for registration:
  - **Explicit mandates**: Impose a penalty for failing to register
  - **Implicit mandates**: Require registration to access essential services

- To avoid implicit mandates, **alternative options for accessing essential services should be available** for those who have not registered

Contents

Digital ID as a priority

Privacy and data protection

Inclusion

Design

Legal assessment

Basic design elements

- There are **multiple valid models** for foundational digital ID systems
  - **Centralized systems**: Often using a single provider to administer the system (India, Estonia)
  - **Federated systems**: Allow multiple entities to provide government-recognized digital ID, with coordinated or accredited by some central mechanism (UK, Canada)
  - **Open market systems**: Multiple regulated entities provide a range of functional IDs and/or civil registers (USA)

- ID systems should be **technology-neutral and vendor-neutral** to keep flexibility and minimize costs

- **Privacy, data protection, non-discrimination and other accessibility elements** should be incorporated into the ID system design

- An ID system should be be **financially sustainable**, with sufficient appropriations/revenue that do not impede inclusion (e.g., fees for individuals for expedited services, fees on third parties for authentication)

Role of the private sector

- The **private sector can be leveraged** in an ID system's design

- **Outsourcing** is a means of using the private sector to carry out discrete tasks, such as registration. To mitigate risks:
  - **Proper credentialing and oversight** is necessary
  - Government should **retain ownership of all data**

- **Public-private partnership arrangements** can be used to procure significant portions of or an entire ID system:
  - Partner selection should use **transparent, competitive and accountable procurement processes**
  - Care must be taken to **avoid vendor lock-in**
  - Partner **revenue streams must not impact inclusion** (e.g., through high fees)

Design sequencing

- While the precise sequencing will vary from country to country, **ID system procurement and design should be informed** by the intended uses of the system and necessary safeguards for privacy, data protection and inclusion

- **Appropriate enabling legal frameworks should be in place** prior to implementation of an ID system to provide necessary protections

- The ID system design should be **designed with constitutional and other privacy protections in mind** to avoid judicial constraints or invalidation
    - aspects of national ID systems have been declared unconstitutional and suspended in some countries

Contents

Digital ID as a priority

Privacy and data protection

Inclusion

Design

Legal assessment

ID4D Diagnostic

- ID4D country engagement to support development of national, digital ID typically begins with a **"diagnostic"**
- Structured **evaluation of a country's current and planned identity ecosystem**, including:
  - Foundational systems (e.g., civil registration, national ID)
  - Key functional ID systems (e.g., voter registration, social protection registers, tax databases, passports)
- Organized according to the **10 Principles on Identification for Sustainable Development** developed by the Bank and partner institutions

ID Enabling Environment Assessment (IDEEA)

Role in Country Engagement

Supplementary tool to the ID4D Country Diagnostic focusing on the **country's legal and regulatory framework** in context of existing ID systems.

Objective

Gather information to enable analysis of legal strengths, gaps and areas for reform.

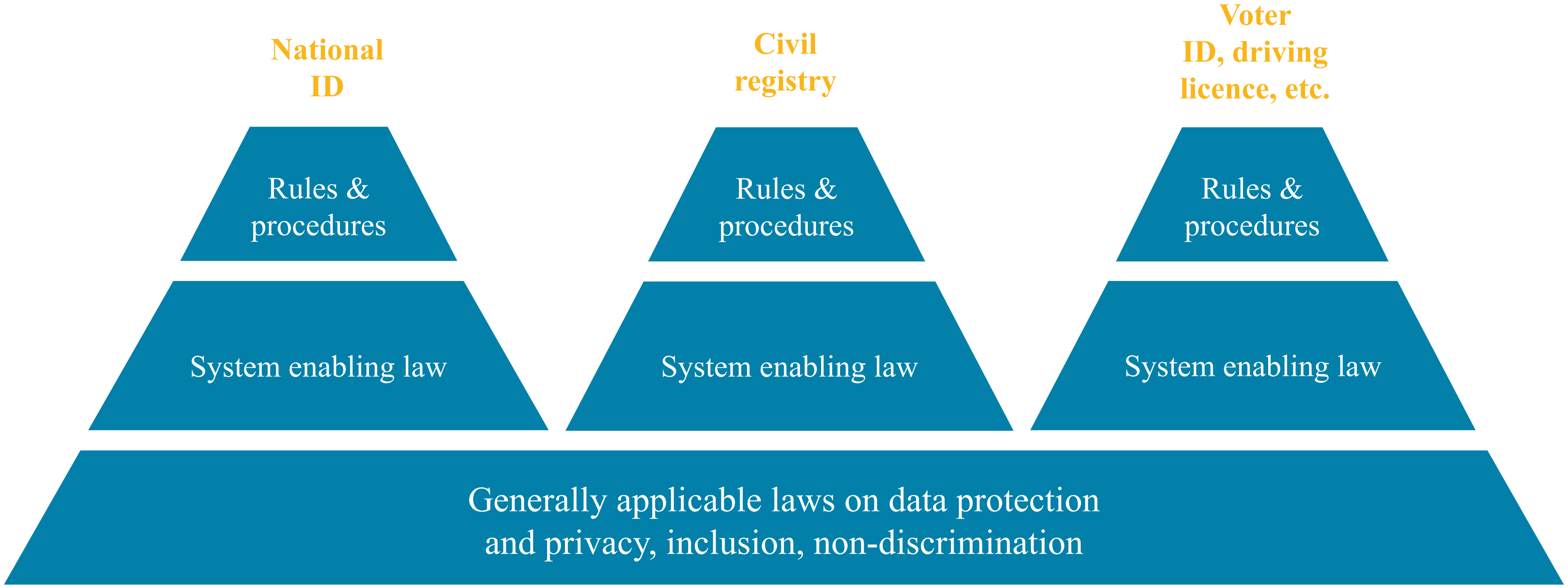
Form

Due diligence checklist questionnaire on the country's existing ID systems, laws, regulations and institutions; and "Y/N" questions supplemented by lengthier explanations.

Focus Areas

✓ Data protection and privacy laws and institutions
✓ Inclusion and non-discrimination laws
✓ Existing ID systems' designs, capabilities, uses, institutional and governance arrangements, and their legal framework

IDEEA’s Scope of Review is multifaceted



National ID

Rules & procedures

System enabling law

Civil registry

Rules & procedures

System enabling law

Voter ID, driving licence, etc.

Rules & procedures

System enabling law

Generally applicable laws on data protection and privacy, inclusion, non-discrimination

- Assessing a country’s readiness may require looking **at each key system’s laws** and regulations as well as **generally applicable laws**
- As digital ID is increasingly used for ecommerce, financial and other digital services, the **range of relevant areas** is potentially endless

- Countries may vary in having one or more, separate or linked, foundational and (key) functional ID systems
- Each may have its own enabling law and rules and procedures
- One or more might be a good base for a national, digital ID
- One or more may already have grappled with key legal and regulatory issues

Structure of the IDEEA

PART I: The country's ID System Landscape

Identifies existing foundational and key functional ID systems

- Civil registration system
- Other foundational ID systems
- Key functional ID systems (including voter ID) which have potential to be expanded for general ID purposes

PART II: Questions about generally applicable regulations

Explores existing legal frameworks and institutions governing:

- Data protection and privacy
- Cyber threats and cybercrime
- International and extraterritorial issues
- Inclusion and non-discrimination

PART III: Questions about each foundational and key functional ID system and its legal framework

Assesses each relevant ID system separately

- Purpose and capabilities of the ID system
- Design of institutions and organizations involved
- Levels of and barriers to participation
- Registration and enrolment process
- Use, storage and protection of personal information
- Individual rights and protections (consent, access, rectification, deletion)

ANNEX I: Questions about governance, social and cultural factors

Addresses broader topics some of which would normally be covered by an ID4D Diagnostic

(To be completed only if no ID4D Diagnostic has been carried out for the country)

IDEEA’s Primary Outputs

A completed IDEEA provides:

A snapshot of existing functional and foundational ID systems including:

- ✓ basic design and functionality
- ✓ institutional structure

An initial review of the trust framework, which can be used to identify risks, gaps and weaknesses.

A map for evaluating potential developments or investments in ID systems and whether the legal and regulatory framework requires:

- ✓ incremental improvements
- ✓ substantial reforms
- ✓ to be built from scratch

Ultimately, the IDEAA can be used to produce a standardized input for gauging countries’ readiness for national, digital ID systems

IDEEA’s Primary Outputs

A completed IDEEA provides:

A snapshot of existing functional and foundational ID systems including:

- ✓ basic design and functionality
- ✓ institutional structure

An initial review of the trust framework, which can be used to identify risks, gaps and weaknesses.

A map for evaluating potential developments or investments in ID systems and whether the legal and regulatory framework requires:

- ✓ incremental improvements
- ✓ substantial reforms
- ✓ to be built from scratch

Ultimately, the IDEAA can be used to produce a standardized input for gauging countries’ readiness for national, digital ID systems

Thank You

THE WORLD BANK