ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

DELIVERY

The following organizations contributed to the development of the Identification Systems for Social Protection tool:

Center for Global Development
Inter-American Development Bank (IDB)
International Labour Organization (ILO)
The World Bank Group (WB)
World Food Programme (WFP)

© 2016 Inter Agency Social Protection Assessments Partnership

The World Bank, 1818 H Street, NW, MSN G8-803, Washington, DC 20433. Telephone: 202-473-7339; Internet: www.ispatools.org

Inter Agency Social Protection Assessments (ISPA) tools have been developed through an interagency effort aimed at supporting policy makers and other stakeholders to gain insights regarding the performance and potential ways to improve social protection systems, programs, and delivery systems. The findings, interpretations, and conclusions expressed in this technical document do not necessarily reflect the views of the ISPA partner organizations or the governments they represent. ISPA does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of the ISPA partner organizations concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Exclusion of Liability: The agencies and authors make no warranty, guarantee, or representation, either expressed or implied, regarding the tools, including their quality, accuracy, reliability, or suitability, and hereby disclaim any warranty regarding the ISPA tools' fitness for any particular purpose. There is no warranty that the tools (or accompanying documents) are free from errors, defects, omissions, worms, viruses, or other elements or codes that manifest contaminating or destructive properties. In no event shall agencies or the authors be liable for any damages in connection with or resulting from the download, use, misuse, reliance on, or performance of any aspect of the tools including any instructions or documentation accompanying the tools. The agencies and the authors make no representation or warranty of non-infringement of proprietary rights of others with respect to the tools. The entire risk as to the uses, outputs, analyses, results, and performance of the tools is assumed by the user.

Rights and Permissions: The material in this work is subject to copyright. Because ISPA encourages dissemination of its knowledge, this work may be reproduced, in whole or in part, for noncommercial purposes as long as full attribution to this work is given. No commercial use, reproduction, or distribution is permitted whatsoever.

ISPA tools are living documents that will be continuously revised based on experiences with their application. Should you have any suggestions, feedback or comments to improve the tools, please contact the ISPA coordination team at info@ispa.org.

Photo: © World Bank
Design: District Design Group
Layout and editing: Nita Congress

ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

DELIVERY

Master Table of Contents

Acknowledgments iii

About ISPA iv

Foreword v

Abbreviations vi

"What Matters" Guidance Note GN-1

Introduction GN-3

1 Conceptual Framework for ID Systems in SP GN-5

2 How Can Countries Improve SP ID Systems? GN-15

3 How to Assess SP ID Systems GN-23

Annexes GN-37

A. General Principles for Privacy and Data Protection in ID Systems GN-38

B. Institutional and Implementation Considerations GN-50

Bibliography GN-65

Questionnaire Q-1

Overview of Findings M-1

Country Report Outline O-1

Acknowledgments

This tool was prepared by a Working Group from the Inter Agency Social Protection Assessment tools initiative led by Robert Palacios (World Bank Group). It has benefited from the input of several experts in the field, including Alan Gelb (Center for Global Development), Mia Harbitz (Inter-American Development Bank), Joseph Atick, William Reuben, and Wyly Wade (consultants) as well as Christina Behrendt, Thibault van Langenhove, and Veronika Wodsak (ILO Social Protection Department). The World Bank's Identification for Development (ID4D) Working Group contributed comments and its global database. Finally, international organizations including the Inter-American Development Bank, the International Labour Organization, and the World Food Programme provided extensive and very useful comments and suggestions.

The Working Group is indebted to officials from the governments of Morocco and Peru where the tool was field tested. They and their teams in Rabat and Lima, respectively, were essential in providing the opportunity to test and refine the tool's first version.

This work has been supported by the World Bank's Rapid Social Response Program, which is supported by Norway, the Russian Federation, Sweden, and the United Kingdom.

About ISPA

The **Inter Agency Social Protection Assessments (ISPA)** tools are the result of a multi-agency initiative that aims to put forth a unified set of definitions, assessment tools, and outcome metrics to provide systematic information for a country to assess its social protection system, schemes, programs, and implementation arrangements. Assessments are done with the goal of improving performance and analyzing trends over time. The ISPA tools are part of a free and publicly available platform, building on existing work by the United Nations system, the World Bank, bilateral donors, and other development agencies.

Within the context of ISPA, **social protection** refers to the set of policies and programs aimed at preventing or protecting all people against poverty, vulnerability, and social exclusion throughout their lives, with a particular emphasis toward vulnerable groups. Social protection can be provided in cash or in kind through noncontributory schemes providing universal, categorical, or poverty-targeted benefits such as social assistance; contributory schemes, with social insurance the most common form; and by building human capital, productive assets, and access to jobs.

Application of the ISPA tools should be conducted at the request of the government and involve all essential national representatives of stakeholders, including the relevant government ministries and agencies, social partners, civil society organizations, national social protection practitioners, and academic experts. They will work together with partner international agencies and other external advisers. ISPA tools are meant to identify strengths and weaknesses of social protection systems and enable governments to identify a set of entry level reform options based on global best practices.

This tool is not intended for use in cross-country comparisons. It is one of the ISPA tools that takes an in-depth assessment at the **DELIVERY** level of analysis. It is complemented by more assessment tools operating at the **SYSTEM** level or looking into specific **PROGRAMS**.

SYSTEM

Assess the social protection system and policies in a country

PROGRAM

Deeper analysis on the different types of social protection programs and branches

DELIVERY

In-depth analysis of different implementation aspects

Foreword

This Inter Agency Social Protection Assessments (ISPA) tool provides guidance on information collection and performance assessment of identification systems for social protection.

The Identification Systems for Social Protection tool is not prescriptive and does not provide a specific implementation plan. It is meant to be a diagnostic tool for application by a team of professionals with expertise in the subject matter. The tool is a living document and may be refined over time.

Like all ISPA tools, the Identification Systems for Social Protection tool includes four parts:

1. The **"What Matters" Guidance Note** provides background for those wishing to carry out or commission a country or program assessment for one or more public works programs. The set of criteria described in the "What Matters" Guidance Note lays down the conceptual foundation for the assessment on the basis of good practices and illustrations from real world experiences.

2. The **Questionnaire** is designed to collect quantitative and qualitative information on social protection system attributes and on some key social protection programs. Its structure and content correspond to the Guidance Note.

3. The **Overview of Findings** helps to organize the findings from the Questionnaire. It uses a four-point scale. The assessment approach helps to identify social protection areas that may benefit from strengthening or are in line with good practices, as well as ensuring that trade-offs between criteria are explicit to policy makers.

4. The main deliverable of an ISPA assessment is the **Country Report**. This document presents the findings, highlights strengths and weaknesses in relation to good practice, summarizes the complex landscape of policies and institutions, and serves as the common starting point for future dialogue between stakeholders.

Abbreviations

CPO	chief privacy officer
CRVS	civil registration and vital statistics
EU	European Union
FIPs	Fair Information Practices
ID	identification
ISPA	Inter Agency Social Protection Assessments
PIN	personal identification number
SP	social protection

All dollar amounts are U.S. dollars unless otherwise indicated.

ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

"WHAT MATTERS" GUIDANCE NOTE

DELIVERY

Guidance Note Contents

Introduction GN-3

1 Conceptual Framework for ID Systems in SP GN-5

A. Why Is Identification Important for Social Protection Systems? GN-6
B. Functional and Foundational IDs. GN-7
C. The Importance of Civil Registration Systems GN-9
D. ID Process for SP Programs: An Overview. GN-11

2 How Can Countries Improve SP ID Systems? GN-15

A. Costs GN-18
B. Risks GN-20

3 How to Assess SP ID Systems GN-23

A. The Questionnaire. GN-24
Module 1: Background Information and Scope of the Assessment GN-24
Module 2: Civil Registration and National ID System GN-25
Module 3: Functional ID Systems. GN-26
B. The Assessment Criteria. GN-27
Criterion A: Coverage and Accessibility GN-27
Criterion B: Robustness of the System and Its Information. GN-29
Criterion C: Costs GN-31
Criterion D: Coherence, Interoperability, and Integration GN-32
Criterion E: Governance and Respect for Rights and Dignity . . GN-33

Annexes. GN-37

A. General Principles for Privacy and Data Protection in ID Systems GN-38
B. Institutional and Implementation Considerations GN-50

Bibliography. GN-65

Introduction

In modern society, individuals need to prove their identity for a wide range of activities including voting, opening a bank account, buying or inheriting property, paying taxes, enrolling in a health insurance plan, or qualifying for a cash transfer. Governments need good identification, and civil registration and vital statistics systems in order to plan and implement public policies effectively—in particular, those related to services and infrastructure—prevent fraud, and track progress in areas such as maternal and child mortality.

For social protection and labor systems, identification (ID) is the cornerstone of any well-functioning program. However, ID and civil registration systems cover only a fraction of the population in low- and middle-income countries. While rich countries have managed to confer legal identity to the vast majority of their populations starting at birth, low coverage in poor countries has resulted in an "identity gap" (Gelb and Clark 2013). This poses challenges for implementation of social protection schemes and programs, which require verifying the identity of beneficiaries as well as—in many cases—their age, address, and family status. National ID systems can greatly reduce the administrative work involved in the ID process for social protection programs. Where no national ID systems exist, alternative mechanisms have to be found; these can either be program-specific mechanisms for beneficiary ID and eligibility verification, or integrated registries to keep records of beneficiaries accessing various programs. Compared to program-specific mechanisms, single registries reduce administrative costs, ensure complementarity of benefits and services, and enable monitoring of the accumulation of benefits within households. Depending on the country context, it may be more appropriate to prioritize building program-specific IDs, integrated registries, or national ID systems.

The spread of national ID systems has been dramatic throughout the developing world, especially in Africa. However, many of these programs suffer from logistical challenges in their implementation, resulting in large coverage gaps. Ideally, these new national IDs could be harnessed by social protection and labor programs, but this is often not the case due to a lack of coordination and long-term planning.

The goal of this tool is to help countries improve their social protection systems. It aims to analyze the strengths and weaknesses of ID systems, with a view to their optimal use in implementing social protection programs.

This guidance note also reflects on the risks involved in ID approaches. The risk of mismanaged procurement or corruption is real and has been documented. The same is true of cases of exclusion, where an ID system allowed governments to discriminate more efficiently against noncitizens or other groups. Finally, an ID system that allows

for certain links to be made easily between databases can exacerbate existing gaps in terms of personal data protection.

This guidance note provides key information and definitions, lays down a conceptual framework, and defines criteria for assessing the performance of existing ID systems. It is accompanied by a detailed questionnaire that is intended to help gather the factual information to be used in evaluating both the national ID ecosystem and the ID process used by particular social protection programs. The questions are meant to facilitate the collection of data, but the questionnaire should not be interpreted as exhaustive in and of itself. Early experience confirms that those conducting the analysis will inevitably encounter complexities and idiosyncrasies that should be further explored in order to understand and fully document the country-specific context.

The analysis should be captured in a country report that should include basic information about foundational IDs and, depending on the focus of the analysis, the ID systems used in specific social protection programs. The Overview of Findings included in this guidance note can be used to provide an overview of the strengths and weaknesses of a given ID system, as compared to defined criteria presented in this note.

1 Conceptual Framework for ID Systems in SP

A. Why Is Identification Important for Social Protection Systems?

The ability to identify beneficiaries is fundamental for social protection (SP) programs to ensure access to entitlements, a well-functioning delivery system, and program sustainability. At both the national and program levels, sound identification (ID) systems increase the efficiency of the overall SP system and the portability of benefits.

Poor ID systems result in exclusion, as otherwise eligible people are not able to access government programs because they do not have the necessary means of ID or because the ID process is too onerous and costly for them. For example, in Peru, where national ID coverage is very high (around 95 percent), a recent study showed that 15 percent of those eligible for a cash transfer program were unable to receive it because they did not have the national ID. In the Dominican Republic, one-third of otherwise eligible individuals were not able to receive cash transfers because they lacked ID documents (World Bank 2007).

A wealth of evidence shows that the poor disproportionately lack forms of ID and that this effectively excludes them from many aspects of social and economic life (Harbitz and Boekle-Giuffrida 2009). It also may prevent their benefiting from SP programs targeting the poor and vulnerable. This becomes a particular issue for children, as programs providing cash, food, and health care, among other benefits, may be linked to nutrition and education programs that disproportionately affect children. Children are particularly vulnerable to exclusion in countries with weak civil registries and low rates of birth registration, which are often associated with low institutional birth rates (see "C. The Importance of Civil Registration Systems"). Moreover, preventing trafficking and child labor depends on authorities being able to identify and track individual children. Other groups that often do not possess forms of legal ID include migrants and refugees, indigenous people, and women—as well as members of other vulnerable groups such as the physically or mentally challenged and the illiterate.

At the same time, the inability to verify identity can result in leakages from SP programs. Fraud can take place when an individual pretends to be someone else either by using a counterfeit ID or an authentic ID belonging to another. India found that ghost beneficiaries of subsidized fuel accounted for 50 percent of actual beneficiaries, leading to a substantial loss (Barnwal 2015).

While there is a need for robust IDs within the context of a particular program, there are also large potential gains from interoperability of the ID system across public programs. The ability to match individuals across databases can reduce costs to

both the government and the beneficiary by eliminating unnecessary duplication of effort (to assign and maintain the ID and for the beneficiary in making multiple enrollments). In other cases, it can make the scheme more efficient; for example, an ID that is accepted by the banking system for know your customer (KYC) purposes can facilitate paying cash transfers or pensions directly into bank accounts. At the system level, interoperable databases may allow for a better design of the overall system architecture, ensuring complementarity of benefits and services and better planning of multiple eligibility for benefits at the household level—thereby avoiding unintended "double dipping." And, to the extent that programs are administered by local or state authorities, interoperability at the national level can facilitate the portability of benefits across the country. Such portability is particularly important in larger countries and for those in the process of urbanization or with significant internal migration, such as China and India.

The benefits of integrated systems need to be weighed against the risks, particularly with respect to regulating access to the data and ensuring privacy, confidentiality of personal information, and data protection (see annex A). In integrated systems, it is more difficult to ensure that the data and information collected are used only for the purposes intended and that data are not stolen, misused, or accessed against the interest of the individual. Ideally, interoperability and data sharing should be limited to the absolute minimum necessary. This means, for example, that the data sets used for ID purposes by various users across the system should be accessible and stored separately from other sensitive personal information related to SP purposes (e.g., personal sociodemographic data on income, health, employment, etc.). An appropriate legal framework should be developed and enforced to minimize data abuses, which is particularly important when it comes to sharing information with private actors. Also, integrated ID systems can create stronger exclusionary effects. An individual who is not included in the integrated system would be excluded from all the programs linked to this single registry.

B. Functional and Foundational IDs

Recognition of the importance of sound civil registration and ID systems has prompted strong interest and resulted in dozens of major projects. In some cases, governments are working with international donors to address a specific need, such as the creation of an ID mechanism to serve a particular program such as health insurance; in other cases, the objective is to create a national ID covering the entire population. These objectives are referred to as **functional** and **foundational** IDs, respectively (Gelb and Clark 2013).

The results of many of these efforts have been less than positive. Donor-driven projects promoting costly technology that do not meet the actual needs of the country but benefit the foreign companies procuring the technology, duplication of effort across government, poor project management, and corruption have resulted in billions of dollars being wasted. Yet better forms of both functional and foundational IDs are potentially extremely beneficial for the population, especially the poor.

The decision to use a foundational ID system for delivering SP (as in Thailand), or to create a functional ID system dedicated to SP (as in Brazil or France) is a political one. The decision made depends on which solution is expected to lead to the best results in the context of how the ID system is to be used, but should also take into account such issues as

- exclusionary effects, particularly with regard to poor and vulnerable populations including women, children, indigenous people, rural residents, the illiterate, non-nationals etc.;
- the cost of registration for an individual;
- the risk of data abuse and discrimination;
- the risk of mismanagement and corruption;
- the cost to the government of introducing and maintaining the ID system.

Institutional capacities, infrastructure, geographical constraints, and cultural factors also play a role in identifying appropriate ID solutions for SP programs. In some cases, a functional ID can grow into a foundational ID, as in the case of the Democratic Republic of Congo—or, some would say, the United States.

The development of a functional ID system often generates a duplication of effort, requiring individuals to have to register twice: both with the functional and the foundational system. Nevertheless, there may be circumstances where functional IDs for SP or other programs may be the appropriate focus for improvement—e.g., where there are concerns regarding human rights if foundational IDs were to be used by programs without appropriate safeguards,[1] or where foundational IDs were simply nonexistent or were unavailable to the poor. In these cases, the best option

1 Of course, functional IDs can also be misused—e.g., by including information that would allow for discrimination on the basis of religion or ethnicity.

available may be to introduce or improve a functional ID that is specifically used by a program, and to consider options to develop interoperable functional ID systems across various programs such as single registries. The standards used at the functional level should be uniform rather than having each program create a new ID silo in order to avoid duplication of effort and to develop synergies. Again, note that it is more difficult to ensure confidentiality of private information, avoid data theft or misuse, and adequately regulate access to data in integrated systems.

On the other hand, the expense and complexity of managing a robust ID system make it very difficult for an individual program to handle it in a cost-effective manner, especially where deduplication is required to ensure uniqueness (i.e., that each individual is entered only once into the database of the ID system).

C. The Importance of Civil Registration Systems

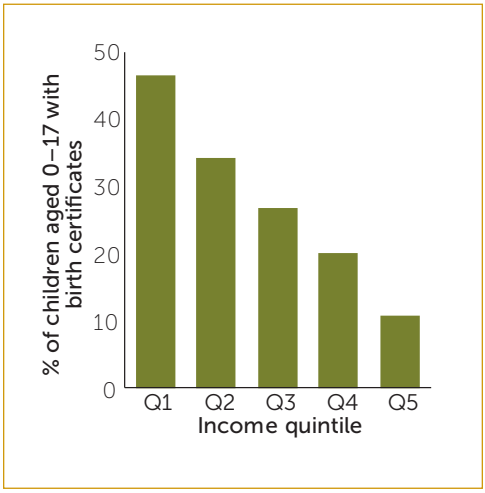
Parallel to the development and improvement of functional and foundational ID systems, important strides are being made in improving civil registration and vital statistics (CRVS) systems.

The link between civil registration and ID is increasingly recognized to be crucial. First, civil registration documents such as birth certificates are, more often than not, the basis for issuing IDs. The birth certificate serves as a "breeder" document in many countries at the point of national ID enrollment or for functional IDs. For SP programs with eligibility criteria related to age (e.g., child benefits or old age pensions), birth certificates enable beneficiaries to prove their eligibility. In the case of migrants, special attention is needed to provide them with documentation and officially recognized legal identification. Registering deaths is equally important, both for national ID systems in general and for SP systems in particular.

But in many countries, most births and deaths are unregistered. A recent estimate is that births are registered for less than 40 percent of children in developing countries. Not surprisingly, this figure is higher in poorer countries, and the poor within all countries are less likely to have births or deaths registered. For example, in Tanzania, the richest households are 12 times more likely to have birth certificates than the poor (UNICEF 2012). And in Indonesia, the rich are four times more likely to register (figure 1.1).

In the vast majority of countries, there are legal mandates for parents to register their children at birth. In principle, this would yield a legal ID document—a birth certificate—for everyone born. In reality, the enforcement of such legal provisions is difficult,

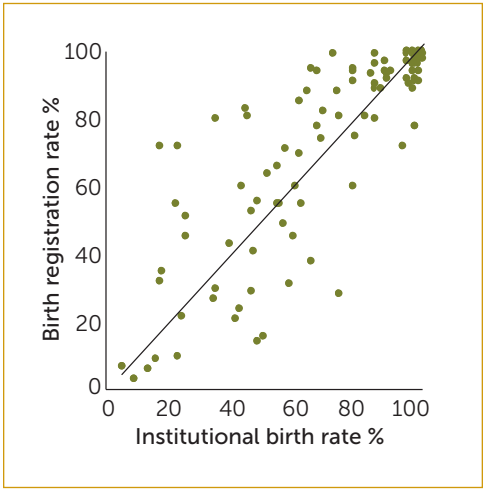
Figure 1.1 Relationship between Income and Birth Certification in Indonesia



Source: Australian Aid 2014.

Note: Quintiles are displayed from richest to poorest.

Figure 1.2 Institutional births and birth registration



Source: UNICEF 2010.

leading to a massive gap between the number of children born and the number registered (figure 1.2). Where ID systems build on CRVS systems, specific provisions should therefore be made for those who do not possess any civil registration document so that those not registered at birth are not also excluded from the national ID system.

Figure 1.2 shows that the wide disparity in birth registration across countries is closely related to the institutional birth rate. However, it also shows that there are countries significantly above and below the fitted line, which raises the question of what else is affecting these rates. Countries with low birth registration and low institutional birth rates in the bottom left quadrant of the figure are unlikely to be in a position to improve their civil registration systems in a way that allows them to rely on it for ID purposes in the near future. Even with rapid improvements in birth registration, the challenge of including the current unregistered population in the ID system persists.

In contrast, countries in the top right quadrant of the figure (those with high birth registration and high institutional birth rates) may be able to close the gap relatively quickly and create strong links between their civil registries and national ID systems. While both areas merit greater attention, a realistic national plan must recognize these limitations.

Some countries have been successful in improving their civil registries. In just one decade, India appears to have increased its birth registration rate by 20 percentage points, from about 60 to about 80 percent. According to United Nations Children's Fund (UNICEF) statistics, several African countries, including Ghana and Senegal, have shown impressive gains over the last two decades; the Philippines has reached a birth registration rate of 93 percent.

The complementarity of the parallel efforts to improve ID systems and civil registries becomes clearer when considering the need to ensure that children are identified properly. National or functional IDs are generally for adults; e.g., voter registration cards. If the birth registration process can be linked to the national ID card, the loop is closed. Many social programs are aimed at children and households and thus require the kind of information that is only captured in the civil registration process. Some countries, such as Uruguay, have closed this loop by assigning a national ID number at birth and by thus linking information flows. The high institutional birth rate in Uruguay allows this link to be made easily (IDB 2011).

D. ID Process for SP Programs: An Overview

There are many different choices regarding the methodology and technology for carrying out an ID system, whether for SP programs or for foundational ID systems in general. Individuals can be identified based on something they **have** (a card, birth certificate, or token), something they **know** (a personal identification number [PIN] or password), something they **are** (biometrics), or because they **are known** (by other members in the community). Many systems combine two or more of these methods of ID to make the system more robust.

Implementing the introduction of a new or upgraded ID system at the national level or for a specific program requires significant resources and planning. It is typically a multiyear exercise that is likely to involve complex procurement, piloting and testing, the capture of key information from individuals, the creation and maintenance of a sophisticated data warehouse, delivery of physical forms of ID, and the development of processes and infrastructure that allow a program or multiple programs to use the ID for authentication. Legal considerations regarding privacy, data sharing, and security are also important elements of an ID system. While implementation processes and structures will differ in their details, all ID systems aim to (1) establish a process by which (either a certain group of or all) individuals in a given catchment area are known; and typically (2) provide individuals with a unique identifier (e.g., an ID number) that allows an individual to be identified, meaning that the person can prove his or

her identity. Generally, this process includes the following steps (for a more detailed discussion of institutional and implementation considerations, see annex B).

1. **Capture: Registration/data collection.** Data on individuals to be identified need to be collected. Acknowledging someone as being entitled to receive an SP benefit requires documenting that person's identity. Documentation is of course a continuous process as new people qualify for SP entitlements, but a large registration effort is needed when setting up a new ID system to capture the entire target population. This process is even more complex for foundational ID systems that aim to capture all citizens living in the territory. The data to be collected need to be carefully defined in advance based on the purpose the system is expected to serve. Decisions need to be made on the type of demographic data to be collected and whether the system will also include biometric information. In the interests of efficiency and data protection, the data collected should be confined to the minimum necessary for the system to perform its function. The method chosen and infrastructure put in place for data collection require careful consideration, since they will greatly influence the accessibility and inclusiveness of the ID system (see the discussion on the accessibility criterion for more information). Besides the data collected from each individual, SP programs will typically enter additional information for each individual in the database, generally including information related to benefit entitlements, eligibility criteria, duration of benefit, conditionalities, etc.

2. **Assigning an identifier.** An identifier is either immediately assigned when data are collected from the individual or once the data set is entered into the database. The identifier consists of the unique variable(s) that is linked to the data set of one individual (one-to-one correspondence). This identifier is often a number or, in the case of biometric IDs, the image/template of the biometric (fingerprint, iris, or facial scan).

3. **Database management.** The data need to be recorded, cleaned, and stored. In addition to general concerns regarding the security, accuracy, and currency of the database, a key consideration in maintaining ID system databases is avoiding duplication—i.e., entering the same person twice. Depending on the methodology and technology used, there are different possibilities for deduplication and for improving the quality of the database; these have different implications and trade-offs, which are presented in the discussion of the robustness criterion.

4. **Authentication.** For many SP programs, individuals need to prove their identity at the point of service delivery or when receiving a benefit. This process of

authentication—of verifying that a person is who he or she claims to be—is done in many different ways, ranging from the simple testimony of other community members to biometric verification matching, e.g., a person's fingerprint to the data stored in the database. Often, a token (an ID card) is issued to facilitate the authentication process. A variety of cards exist (standard paper or photo ID, barcode, magstripe card, chip card, etc.) which differ in terms of their costs, data storage capacity, security, infrastructure needs, and so on. Their respective advantages and disadvantages are discussed in table 2.1. Passwords or codes can be used to create an additional layer of security. Again, there are various trade-offs regarding cost, accuracy, user-friendliness, considerations regarding the rights and dignity of beneficiaries, and technology reliability that need to be carefully weighed against each other to determine the appropriate authentication process. Systems relying on high-tech methods are well advised to have a backup solution for identity verification, as technology is prone to failures due to connectivity problems (in the case of systems operating online), power cuts, etc. The identifier needs to be delivered (in the case of a card) or communicated to the person (in the case of a code or password), and the infrastructure for authentication installed at the points of service or benefit delivery.

5. **Update/renewal.** Most ID systems require periodic verification of the data in the system. In the case of systems that issue ID cards, these typically have to be renewed periodically. In many SP programs, this process will also entail verification of whether an individual continues to meet the eligibility criteria and is thus still entitled to receive benefits.

2

How Can Countries Improve SP ID Systems?

There is no one correct path toward setting up an ID system for SP. Some countries may further develop existing functional ID systems applied to specific programs and expand their use and coverage over time. Others may adopt a top-down approach that puts in place a foundational ID that can be used by individual programs. There are different initial conditions, political priorities, and varying capacities to implement an ID system, all of which influences decisions on how to move forward. Some interim ID mechanisms may be required in order to move ahead with the implementation of a particular program, since access to social and anti-poverty programs should not depend on a country having a national ID system in place. In countries with no widespread national ID system, SP programs rely on the creation of functional ID systems to ensure benefit delivery. If well designed and implemented, the system can serve the purposes of the program in question even in the absence of a foundational ID system. In fact, it may even become the basis for a foundational system over the long run.

Where different programs have led to the development of multiple ID mechanisms with reasonable accessibility and robustness, these can be built on to improve interoperability if individuals in the different databases can somehow be mapped to each other. However, this normally requires a common identifier. The caveats cited earlier regarding personal data protection must be kept in mind, and the data accessible through the common database be limited to the minimum.

In some cases, it may make sense to improve upon a foundational ID system that already has good coverage or accessibility and improve its robustness by shifting to a new technology such as biometrics (box 2.1). This is the approach planned in Egypt, where birth registration rates are reported at 99 percent and coverage of a nonbiometric ID assigned at birth is high. Replacement IDs will eventually be based on new, biometrically deduplicated ID numbers. Building an ID system for SP programs on such national ID systems will reduce the administrative costs and leakages of the SP programs. To ensure confidentiality of private information, it is good practice to store the SP-related information in a separate database and limit the use of the national ID to the initial enrollment/ID purpose.

In other cases, countries have opted for a sudden and discrete shift to a new ID paradigm that can then be adopted by individual programs. India and Pakistan are currently taking such an approach. In Pakistan, a national ID is a relatively recent development, but it is now the basis for that country's largest cash transfer program, the Benazir Income Support Programme (BISP), and is being incorporated into social insurance and other government programs as well. It is also being used for financial sector transactions.

Box 2.1 Advantages and Risks of Biometrics

Digitized biometrics have several advantages over physical tokens and numeric codes, in that they

- are unique to each individual;
- cannot be lost or forgotten, and are very difficult to counterfeit or steal;
- do not require literacy;
- are automated and leave an auditable trail;
- increase anonymity when used in place of personal identifiers (names, addresses, etc.).

At the same time, it is important to recognize the limits of biometric technology and continuing concerns about its security.

- There is a danger of data abuse, especially if biometrics are used in a context where there are no well-developed legal and institutional frameworks to protect rights, personal data, and privacy.
- Some biometrics may not be as stable as originally believed (Fenker and Bowyer 2012). "Spoofing"—counterfeiting biometric measurements—is possible, though it requires sophisticated technology and can be prevented by alert operators.
- Fraudulent biometric IDs can be obtained on the basis of counterfeit breeder documents or stolen data.
- Database theft poses particular challenges, in that once the identifier indicators are compromised, they cannot be reissued as can signatures or passwords. A person cannot change his or her fingerprints or iris if an impostor is using the data.

The relative security of biometrics may also be compromised when combined with other technology—e.g., offline card-based systems, which have been found to be vulnerable to hacking and cloning.

In this context, it is interesting to note that developed countries use biometrics mainly for forensics and security; very few use them for identity systems or public service delivery. In contrast, developing (low- and middle-income) countries are increasingly using biometric technology for civil registries, voter rolls, health records, and SP (Gelb and Clark 2013).

A. Costs

These broad options—as well as many choices regarding the details of the technology and processes—will entail different start-up and maintenance costs. A very important consideration is the cost of achieving accessibility, as the most remote geographic areas and the poorest segments of the population are generally the most costly to reach. But costs vary with many elements of implementation, ranging from the security features of ID cards to the quality, security, and accuracy of authentication devices. The budgetary constraints and opportunity costs of these choices will need to be assessed for the particular country and should become part of the formulation of the national ID strategy. For SP benefits, maintaining a certain proportionality between program objectives, benefit levels, and cost of the ID/authentication solution should be carefully considered.

For card-based systems, costs vary according to the complexity and security of the card chosen. One cost driver is **customization** and **personalization** to make cards more difficult to forge. Customization involves the inclusion of logos, holograms, and certain security features unique to the card but not unique to the person the card is issued to or the agency issuing the card. Customization usually involves features that are printed, etched, or engraved at the factory. Personalization, on the other hand, refers to the items that change when issued to the cardholder, including numbers, demographic data, and photographs. These features are generally printed, etched, or engraved in the country at either a central location or in the field where the card is issued. Personalization features fall into three categories: **human detectable**, **machine detectable**, or **lab verifiable**. The more complex the customization or personalization features, the more card management becomes an issue—and the more likely the card will need to be centrally printed. Including an "antenna" in the card for contactless reading drives up the cost and complexities even further.

Table 2.1 provides an overview of standard card types, their key features, and their main advantages and disadvantages.

Another significant set of considerations is the cost of different options, the risk of overspending on inappropriate technology, and duplication across programs and over time. In international practice, there are many examples of high-cost, proprietary packages being chosen instead of cheaper, standard low-tech substitutes that are often entirely sufficient for the intended purposes. The lack of experience and expertise within governments in specifying needs and in contracting for or procuring needed goods and services—as well as a lack of coordination between programs—has

Table 2.1 Summary of Card Type Features, Advantages, and Disadvantages

Card type	Key features	Advantages	Disadvantages
Standard card	• Printed card with no readable features	• Inexpensive to produce • Easy to operate • No reading hardware required	• Easily forged • No data storage • No possibility to connect electronically to the management information system
Barcode card	• Static scan card • Stores a number linking to a computer system that can be used to verify data on the card or retrieve other information about the cardholder	• Inexpensive to produce • Can be printed on plain paper (card stock is cheapest)	• Barcodes are easily forged and easily damaged; even minor damage can render the barcode nonfunctional • In many developing countries, cardholders laminate cards to protect them, which, in many cases, renders the barcode useless • Barcodes store very little data • Data cannot be rewritten or modified
Magstripe card	• A number encoded on the magnetic strip of the card can be read through magnetic readers. The number is used to pull up a record within a computer application. This application and the database that it is attached to can reside both locally or be online for online processing. • The magnetic strip allows re-encoding only a limited number of times, so these cards are good for static data that does not change. • The data on the strip can be modified and changed by other cards or by getting too close to magnets.	• Low-cost encoding • Cheaper card stock compared to other card technologies • Readers are common • Largely based on international standards	• Magnetic strips are easy to de-magnetize • Life cycle is limited if frequently used • Can only store up to a maximum limit of 2 kilobytes • Requires a computer to link to an application

Card type	Key features	Advantages	Disadvantages
Smart or chip-based card	• Chips enable many more applications but introduce complexities, such as key infrastructure, data size, public and private application data, integrated security procedures and intersectoral/interministerial data-sharing agreements • Smartcards can provide services for both online and offline processing • Possible to store significant amounts of data on the card, meaning a computer application can read and manage the data rather than requiring connection to other systems	• Can dramatically increase security • Allows for both online and offline application usage • Can store many megabytes of data • Cardholder data stored on the card rather than on a computer system • Reader is cheaper than barcode	• Added complexity for issuing group • Cards without covers can be "temperamental," subject to conditions such as dirt and temperature

resulted in parallel, expensive ID systems being purchased unnecessarily, often for the same target population (e.g., the poor).

B. Risks

There are always risks involved in introducing a new system, changing an existing system, or moving from one system to another. These risks must be weighed against the cost of inaction. Risks can be grouped roughly into two categories: the risk of **exclusion** and the risk of **misuse** of databases.[1]

The first category—the possibility of exclusion—applies to any type of change or improvement to an ID system, regardless of whether it is functional or foundational. Shifting from one accepted form of ID for say, a cash transfer, to another requires careful transition planning so that beneficiaries have sufficient opportunity and awareness to obtain a new ID without losing benefits in the interim. Another potential source of exclusion arises if the new system uses criteria for ID eligibility that effectively

1 A third category of risk is generic. Any major change to a fundamental aspect of society entails significant risk of failure due to, e.g., changes in political support, resistance of vested interests, corruption in procurement, and weak capacity for change management.

exclude some individuals—e.g., because they cannot prove that they are citizens (Gelb and Clark 2013).

In addition to potential exclusion, there is a risk of data theft or the misuse of ID databases. In fact, the reluctance in many richer countries to have a robust, centralized national ID system stems from respect for an individual's right to privacy regarding personal information and historical experiences. There have been cases where a link between IDs has been cited as facilitating genocide (EFF n.d.; Fussell 2001; Hu 2013). However, unless the alternative is to forgo the benefits of an ID system, strong safeguards and mitigating measures should be applied to minimize the chances of such abuses. For instance, governments should limit the collection of data to the minimum necessary and avoid the capture of certain information that could be potentially misused (e.g., on race or religion). Moreover, they should limit access to databases based on what different actors require through clear regulations and legislation. These safeguards should be strictly enforced and regularly monitored, and clear lines of accountability should be put in place. Mechanisms for redress in cases of incorrect ID or violation of privacy and confidentiality should be clearly established; these should be impartial, simple, transparent, effective, and accessible free of charge for the applicant.

3

How to Assess SP ID Systems

When assessing ID systems from an SP perspective, the first step is to take stock of the existing system or systems. The collected information forms the basis for a country report that assesses the existing structures, processes, rules, and technology against agreed criteria and elaborates on the gaps and areas for possible improvement in the system(s) of a country or specific program. This Inter Agency Social Protection Assessments (ISPA) tool therefore includes (1) a questionnaire that identifies key areas on which to collect relevant qualitative and quantitative data and information, (2) a set of assessment criteria, and (3) a matrix that provides an overview for assessing each key area against the relevant criteria. This section explains in detail the structure of and rationale behind the questionnaire, the assessment criteria, and the Overview of Findings.

A. The Questionnaire

The questionnaire is divided into three modules; each of these is detailed in the remainder of this section.

1. **Background Information and Scope of the Assessment.** This module sets out the key features of the country related to its ID system(s) and its SP system. It also defines the scope of the assessment (e.g., focus on one program ID system, assessment of the SP system as a whole).

2. **Civil Registration and National ID System.** This module details the functioning of the national civil registration system (if one exists), and summarizes key features and data of the different ID systems existing in the country (both foundational and functional).

3. **Functional ID Systems.** The third module contains questions that should be administered for each functional ID system included in the assessment. It includes subsections paralleling Module 2 aimed at understanding the registration process, database management, administrative framework, security, accuracy, and performance of the system.

Module 1: Background Information and Scope of the Assessment

The objective of this first module is to provide a rapid overview of a country's main SP programs and the ID systems they are using. It is divided into four key areas:

- **Key Area 1: Context of the assessment.** Questions 1–6 gather general information on the assessment process, objectives, involved organizations, and time frame.

- **Key Area 2: Scope of the assessment.** Question 7 aims to precisely define the scope of the assessment in line with its objectives (e.g., identifying the appropriate ID system to be used for a new program, developing a strategy for rationalizing ID systems for SP programs, etc.).

- **Key Area 3: Country background information.** Questions 8—14 elicit basic information on the country that have an impact on the design or performance of ID systems used for SP.

- **Key Area 4: Country background SP information.** Question 15 seeks basic information on the SP context.[1] In addition to a brief description, the following minimum information should be compiled for each program: program name, program typology and duration,[2] objective/target group, managing institution, annual coverage (number of individual and participant households), entitlements (level of wage and other benefits; modality of payment—cash or in kind), and ID system used.

Module 2: Civil Registration and National ID System

The second module aims to gather information on the country's national ID system. A first key area is dedicated to strategic issues, a second to the civil registration and vital statistics system (as discussed earlier, CRVS systems are often the basis for ID systems), a third details the national ID system—foundational (if it exists), and a fourth elicits information on other existing national ID systems. The final key area aims to describe the national framework regarding personal data protection and the use of the national ID to link different databases.

- **Key Area 5: Strategic issues.** Questions 1–5 gather information on the national framework for ID systems. These aim to provide general information on national strategies regarding ID systems and the related institutional setup.

1 For a more in-depth analysis of the performance of the overall SP system, refer to the Core Diagnostic Instrument (CODI) ISPA tool.

2 By typology, the tool refers to poverty and social exclusion (general social assistance), old age, survivors, health, sickness, disability, employment injury, maternity, children/families with children, active labor market programs, unemployment, and other; specify (housing, nutrition, basic education including subsidies, etc.).

- **Key Area 6: CRVS system.** Questions 6–27 seek to describe the way birth and deaths are registered in the country.

- **Key Area 7: National ID system.** Questions 28–73 intend to describe the national ID (i.e., foundational) system. This key area is organized into six parts: overview of the national ID, description of the national ID document and number, issuing agency, enrollment and issuing process, data and deduplication, and uses of the national ID.

- **Key Area 8: Other ID systems at the national level.** Questions 74–81 identify and describe other ID systems at the national level. This subsection also discusses coordination between these national ID systems. Key Area 9: Personal data protection. Questions 82–98 provide an extensive description of national provisions regarding personal data protection and the use of the national ID system to create linkages between different databases.

Module 3: Functional ID Systems

Questions in this module should be answered for each of the functional ID systems included in the assessment. The module is organized according to the assessment criteria and thus, aside from the introduction which collects general information on the ID system as a whole, covers five key areas; these correspond to the five assessment criteria discussed below.

- **Key Area 10 (Criterion A): Accessibility.** Questions 1–33 cover issues such as coverage, the enrollment process and related costs, as well as the inclusiveness of the system.

- **Key Area 11 (Criterion B): Robustness.** Questions 1–24 address uniqueness, credentials, data security, authentication, and database management.

- **Key Area 12 (Criterion C): Costs.** Questions 1–14 cover current information technology costs, maintenance costs, ease of operation and cost of training needs of administrators.

- **Key Area 13 (Criterion D): Interoperability and portability.** Questions 1–14 cover system interoperability and portability.

- **Key Area 14 (Criterion E): Governance.** Questions 1–35 deal with the governance framework, institutional capacity, and respect for rights and dignity.

B. The Assessment Criteria

For convenience, the dimensions on which to assess ID systems can be grouped into five criteria: accessibility, robustness, costs, coherence, and governance. Each of these criteria can be applied to the SP system as a whole as well as to specific programs. They can also be used for assessment of either a foundational ID system or a functional (program) ID system. See the Overview of Findings for guidance on how to use the criteria and assess performance.

Criterion A: Coverage and Accessibility

Accessibility is important in achieving a high level of coverage in a functional or foundational ID system; low coverage is a key indicator that a system is not accessible. For the purposes of this tool, the accessibility of an ID system is assessed by analyzing the population **coverage** of the ID system; the extent to which the system ensures **inclusiveness**, including of vulnerable groups of the population that are difficult to reach; and the **appropriateness** of the arrangements in place aimed at overcoming barriers to access.

Coverage

Coverage can in theory be measured by either comparing administrative data on the number of IDs issued to the potential covered population, or through nationally representative surveys that ask whether births have been registered and if certain forms of ID, including functional IDs, are held. In countries where a national ID number is issued at birth and institutional birth rates are high, such as in France and the United States, coverage is close to universal. Many social programs do not require a national ID, but issue their own form of ID. This may be due to low coverage of the national ID or other considerations such as lack of robustness. In these cases, the relevant indicators are related to the actual coverage of the functional/program ID among all targeted beneficiaries.

Inclusiveness

Inclusiveness is a challenge, particularly in low-income countries where a large percentage of people often do not have any form of ID.[3] An inclusive system should ensure universality, meaning potentially every resident an ID system intends to cover is able to be included in the system. (Certain ID systems are not designed to be universal;

3 In some cases, ID numbers may have been generated but not communicated or distributed to individuals, who thus cannot use them for ID purposes.

e.g., voter IDs are only issued to adult citizens.) Vulnerable groups, especially the poor, and—where ID processes are centralized—the poor living in rural areas, are the most likely not to have been registered and to have difficulty accessing decentralized paper records of their births.[4] The poor may also be less aware of the importance of or need to register, and they may not be familiar with the relevant administrative processes. ID and authentication processes should not create stigmatization and mistrust. If a stigma is attached to holding a particular form of ID, this will greatly discourage enrollment. Inclusive systems communicate effectively to all population groups as to why and how they should obtain IDs. The inclusiveness subcriterion assesses the extent to which coverage of the ID system is particularly low for vulnerable population groups.

Appropriateness

Several factors in the design of an ID system influence its appropriateness in ensuring accessibility. The process of obtaining a foundational or functional ID or registering births may be too costly for the poor with regard to both direct and indirect costs, such as travel and lost earnings. Migrants and other vulnerable groups face additional difficulties in obtaining an ID such as not having a birth certificate. Effective access requires appropriate administrative procedures that should be as simple and quick as possible, ensuring geographical accessibility and overcoming cultural and language barriers. Outreach activities and mass enrollment can improve accessibility for remote areas or marginalized population groups. Mass enrollment campaigns can help accelerate coverage extension, as in Pakistan where an estimated 85 percent of adults have a national ID card. A study carried out in Peru (Reuben and Cuenca 2009), found migration and distance and access to registry offices to be the main factors in explaining low ID coverage among the poor. Even after a successful initial enrollment process takes place, the implementing agency will need to update information and continue to add new individuals. Ensuring consistently high coverage rates may require special, ongoing efforts to reach people, especially in the most remote regions. In Peru, the national ID and civil registration agency has a unit dedicated to reaching people in the country's jungle and mountainous areas, using mobile units and teams knowledgeable in indigenous language and culture.

A passive approach that requires people to come to central locations and involves minimal outreach is at the other end of the spectrum from the mass enrollment approach. In many cases, people must bring additional documentation (e.g., birth

4 The rates of birth registration vary widely by country and are highly correlated to levels of per capita income. See UNICEF (2012), table 9.

certificates) with them for validation. Clearly, this approach tends to exclude the poor for whom the cost of access and information becomes a serious barrier.

Criterion B: Robustness of the System and Its Information

An ID system is considered robust if it ensures uniqueness, i.e., that each person can only register once; security regarding the mode of ID; and sound authentication.

Uniqueness

Perhaps the most important feature of a robust form of an ID number or document (e.g., card) is uniqueness. Assigning a unique number to such a document that corresponds to a unique individual requires a deduplication process—i.e., a check to ensure that no person is entered in the database more than once. While no system can be expected to be without some error, a robust system is one where the error rate is minimal—and, therefore, the chances that one individual has more than one number assigned to him or her, or that a particular number has been assigned to more than one person, are negligible.

Deduplication for large numbers of individuals is difficult without biometrics because many people share the same name and nonbiometric information may be collected multiple times but entered differently. Biometrics, combined with a deduplication technology that allows comparison between database entries, is the most robust way to ensure uniqueness. It can also be expensive; few, if any, program IDs are biometrically deduplicated. Duplications can also be reduced by "demographic deduplication"—i.e., by running smart comparisons of information captured in the database (name/surname, date of birth, address, etc.). This process is not perfect, as misspellings or other data entry errors can ascribe uniqueness where it does not exist. If information cannot be verified separately, a person can fabricate biographical information and create a false identity. However, some countries—such as Brazil with its Cadastro Unico—have achieved a high degree of accuracy in their databases through a deduplication process based on the information captured, without relying on biometrics. While the advantages of having uniquely identified individuals are clear, the cost of ensuring uniqueness must be measured against the benefits for a program that cannot use a deduplicated ID. Conversely, given the expense of deduplication, it would be inefficient and costly at the individual program level.

Security

A robust system is one where identity fraud is very difficult (albeit never impossible). For instance, it is much easier to produce a fraudulent photo ID than a biometrically

verifiable electronic ID. The card itself could also have a number of security features making falsification difficult. Some combination of factors corresponding to biometrics (what you are), PINs or passwords (what you know), and the presence of a card or some other token (what you have) can help deter fraud. Note, however, that biometric ID is not a perfect safeguard against identity fraud. Even if ID cards are not easily falsifiable, they may be fraudulently obtained, using forged or falsely acquired breeder documents (such as birth certificates) unless complex (and sometimes expensive) verification and authentication measures are in place. Again, those administering specific programs must assess the cost of adding these security features relative to the benefits of reducing fraud.

A key concern in this context is database/information security and sound encryption technology, especially if biometrics are used. Biometrics are unique to an individual and are therefore sensitive information that needs to be protected with the highest standard of care to thwart any possibility of theft or misuse.[5] A particular disadvantage of biometric data lies in the fact that once the identifier indicators are compromised, they cannot be reissued as can signatures or passwords: a person's fingerprints or irises cannot be changed if an impostor is using these data. Furthermore, security protocols that ensure backup and restoration routines are necessary for sound system operation, not just to prevent misuse but also to ensure preparedness against technology failures or malware attacks. These controls are discussed in more detail in annex B.

Reliable and Effective Authentication

A program ID may not be robust even if it is deduplicated and has a high level of security if those security features are ignored at the point of a transaction such as a cash transfer payment or receipt of medical attention at a clinic. In this regard, several countries that use expensive and sophisticated smart cards do not take advantage of the information stored on the card which could be used to electronically verify identity and track transactions. Without authentication, an otherwise robust ID could be used by someone other than the intended beneficiary. Failure to identify an individual entitled to a benefit leads to unintended exclusionary effects, while incorrect assignment of benefits means additional costs.

5 Unlike other possible identifiers, biometrics are not provided by a third party nor chosen by the individual. Biometrics are produced by the body itself, and thus belong to the individual generating them. Legally, the human body is an integral part of the person, and all physical information naturally fits into the personal information field. Consequently, biometrics are by nature considered private information.

Incentives, accountability, and well-trained administrative staff are all needed for effective authentication. In addition, software and hardware used for enrollment and authentication is not infallible.

Three types of errors can occur during enrollment and in matching an individual's information against that stored on a card or in a database.

- **Fail to capture (failure to enroll).** An error occurs during the enrollment process; e.g., in a biometric system, the enrollment hardware cannot capture an image of sufficiently high quality.
- **False positive.** The system erroneously finds a match between the captured data and another individual in the database so that someone will appear to have already registered but has not in fact done so.
- **False negative.** The system erroneously finds no match of the captured data in the database, although the person is already registered.

False positive and false negative errors have different consequences (acceptance or rejection), depending on whether they occur in a 1:1 match or a 1:*n* match as follows:

Match	False positive	False negative
1:1	FAR	FRR
1:*n*	FRR	FAR

Note: FAR = false acceptance rate—the rate at which unauthorized individuals are allowed enrollment/access; FRR = false rejection rate—the rate at which authorized individuals are denied enrollment/access.

There is a trade-off between the false acceptance rate and the false rejection rate; algorithms that have a low tolerance for the former will by definition have higher false rejection rates. Thus, each program must balance whether it is more important to ensure uniqueness at the risk of falsely rejecting eligible individuals, or to be inclusive at the risk of falsely accepting ineligible individuals.

Criterion C: Costs

Cost is often a key driver in the actual decision of what kind of ID system needs to be applied. Cost considerations include the following.

- **Infrastructure.** These include the cost of hardware at ID registration points, at service/benefit delivery points for authentication, for database storage; the cost of cards; etc.

- **Operating and maintenance costs.** These include the lifespan of the infrastructure and ID cards, the cost of Internet connectivity, and staff costs to run the system (registration, authentication, database management).

- **Other.** These include the cost of administrator training and the cost of a backup system in case of technology failures.

The complexity (and costs) of the system should be reasonable compared to its intended use. An SP program that delivers food aid in the lean season worth a few dollars per household may not require a very elaborate ID system. However, if there is a plan to issue a single card that enables access to a full range of goods and services, investing in some security features is more justified.

Criterion D: Coherence, Interoperability, and Integration

This criterion assesses to what extent the IDs used in the SP system are based on a coherent and integrated approach that maximizes user friendliness and efficiency while minimizing error, data misuse, and fraud.

The degree of interoperability/integration brings with it the risk of an overly concentrated pool of information, raising questions of privacy and data-sharing regulations and protocols (these are also related to robustness and legal frameworks and data protection). These issues are of particular concern regarding access to databases linked through a national ID number and the potential for misuse of data. Many countries have established elaborate mechanisms to ensure that each agency has only access to a certain minimum amount of data common to all databases (national ID number and some additional variables, such as date of birth and sex), while program-specific information (e.g., employment histories, medical records, etc.) remains with the administering agency and is not accessible by other agencies. Such an approach of strictly regulated access to data seeks to balance the advantages of an integrated system with data protection concerns. This concern is assessed under Criterion 5 (governance and respect for rights and dignity).

Interoperability

Interoperability considerations relate to the extent to which a particular ID can be tracked in different databases. Interoperability can help increase user friendliness and reduce administrative costs and leakage by reducing duplication of efforts and targeting errors. Integration is the use of one ID by many programs and actors, allowing the ID holder to verify his or her identity for many different purposes; in principle, such integration enables relevant parts of different databases to be mapped to each other. For instance, in the United States, a social security number is required for transactions ranging from paying taxes to receiving pensions and health insurance, as well as for private transactions such as opening a bank account. In Costa Rica, a unique number is used with income taxes, property registration, school registration, passports, social security, and driver's licenses as well as all official documents. In Peru, the use of the national ID is mandated for all major transactions and programs.

A more integrated ID can help government map individuals across programs. In Argentina, this kind of linkage between databases through one ID number allowed the government to detect fraud by showing that higher-income individuals, determined based on their tax payments, were also receiving means-tested benefits. In Turkey, data exchange protocols between the social assistance scheme and a variety of other government databases such as land and auto registries are used to improve targeting.

Ubiquity/Portability

Integration can also facilitate transactions taking place across subnational entities, thus ensuring that entitlements or eligibility conditions can be obtained or verified in the case of everyday events such as moving, changing employment, changes in marital status, etc. In India, most program or functional IDs (e.g., ration cards) can be used only at the state or district level, while the Rashtriya Swasthya Bima Yojana (RSBY) health insurance card is unique at the national level and can be used at any accredited hospital across the country.

Criterion E: Governance and Respect for Rights and Dignity

Governance Framework

The roles and responsibilities of the various institutions involved in the implementation and oversight of the ID system must be clearly assigned and communicated through a sound regulatory and legal framework. National stakeholders, including representatives of marginalized and disadvantaged population groups, must be

informed about ID approaches, and their views and concerns taken into account in the design, implementation, and monitoring of ID approaches.

There are different institutional setups for administering an ID system.[6] In some countries, a specialized institution exists that deals exclusively with ID, and arrangements with other government agencies or private sector actors are defined. This is the case, e.g., in India and Pakistan. A less frequently observed case is where both civil registration and national ID management are located within the same institution; this is the case in Peru.

On the other hand, many social programs issue their own forms of ID, often because a foundational ID does not exist or is not considered robust and/or inclusive enough to serve the purposes of the program. In these cases, the form of ID will be administered by the relevant ministry. A commonly observed case is the functional ID of the electoral register. Its breadth of coverage often leads to competition with parallel national ID systems.

If there is a significant degree of integration, the agency administering the common unique ID has an important role to play in personal data protection, even though these rules are enforced by a different part of government. Regardless of the specific setup, clear lines of accountability should be established.

Institutional Capacity

An important aspect in the sound implementation of an ID system is having an adequate level of institutional capacity to roll out the necessary administrative processes (for foundational IDs and national SP programs IDs) and database maintenance effectively and efficiently, respecting the rights and dignity of the population. An adequate number of staff with the right training and skill sets are needed, as well as the requisite infrastructure (computers, printers, and other technological devices; including mobile services to ensure accessibility for populations living in remote areas).

Respect for Rights and Dignity

The Convention on the Rights of the Child confirms the right of each person to an identity and nationality. It also recognizes the right to privacy of personal information,

6 The Inter-American Development Bank has produced an inventory of vital registry and ID institutions across Latin America that includes descriptions of such institutional arrangements.

as do several other human rights instruments, including the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17). The International Labour Organization's Social Protection Floors Recommendation (No. 202, adopted in 2012) sets out that states should establish a legal framework to secure and protect private individual information contained in their SP data systems (paragraph 23).

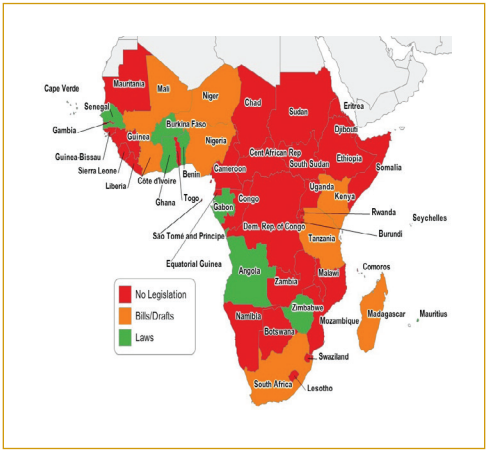
With a view to protecting data and privacy, some countries effectively prevent integration in order to minimize the potential for linking different databases with personal information and thus mitigate the risk of data theft or misuse. In these cases, it is necessary to set up mechanisms that allow these links to be made when needed (e.g., for deduplication) but under clear supervision. In the European Union, this supervisory role is played by a specific agency responsible for oversight of data access across government agencies. Efforts are also under way in countries in other regions to ensure data protection and privacy in ID systems.

There are valid concerns about the misuse of personal data for surveillance and other intrusive practices that could infringe on personal liberties. The poor are especially vulnerable to these dangers, as reflected in the *Guiding Principles on Extreme Poverty and Human Rights*:

> States should: (a) Revise legal and administrative frameworks to protect persons living in poverty from inappropriate intrusion into their privacy by the authorities. Surveillance policies, welfare conditionalities and other administrative requirements must be reviewed to ensure that they do not impose a disproportionate burden on those living in poverty or invade their privacy. (OHCHR 2012, p. 20)

Many countries with national ID systems do not have privacy legislation. This is true for much of Africa, where almost every country has a national ID card (most of which are electronic IDs), but—as shown in figure 3.1—a minority of countries has a regulatory framework to protect personal data.

Figure 3.1 Status of Privacy Rules in Africa



Source: Dener et al. 2015.

Even India, where state-of-the-art technology is being rolled out to more than 700 million people, has not yet put in place the legal and institutional safeguards that would be expected.

The topic of personal data protection and periodic updating is an important consideration when thinking about the integration of identity systems as well as in the legal and institutional setup of ID systems. If biometric data are used, for instance, the data should be stored exclusively as encrypted templates on smart cards or similar devices to allow a standard comparison to be implemented directly on the card/device in question. Avoiding the creation of a database including biometric information limits the risk of identity theft and misuse.

These safeguards should not only ensure the confidentiality of private information but also respect for the dignity of the individuals registered. This entails avoiding stigmatization and discrimination both during the ID process as well as with regard to the information collected.

Well-established internationally recognized Fair Information Practices (FIPs) guide personal data access not only for ID systems, but for any information about individuals that is collected by government. These include guidelines on the limits of data collection; the need to ensure data quality; the need to clearly specify the purposes for which data can be used and to whom it can be disclosed and under what circumstances; safeguards for protecting data from unauthorized access, destruction, modification, or disclosure; transparency of data rules; the right of individuals to challenge and correct their data; and clear accountability of a designated data controller for any breaches of these principles.[7] In short, the legal and regulatory framework that applies to personal data protection is an integral part of an ID system.

For instance, governments should limit the collection of data to the minimum necessary and limit access to databases based on what different actors require through clear regulations and legislation; they should also avoid the capture of certain information that could be potentially misused (e.g., on race or religion). These safeguards should be strictly enforced and regularly monitored. Mechanisms for redress in case of incorrect IDs or violation of privacy and confidentiality should be clearly established and should be impartial, simple, transparent, effective, and accessible free of charge for the applicant.

7 These principles are explained in greater detail in annex A.

Annexes

Annex A. General Principles for Privacy and Data Protection in ID Systems

The principles for privacy and the protection of data are set out in international and regional human rights standards and principles. Specifically, the right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12), the International Covenant on Civil and Political Rights (Article 17), the Convention of the Rights of the Child (Article 16), and the International Convention on the Protection of Migrant Workers and Members of their Families (Article 14). At the regional level, the right to privacy is protected by the African Charter on the Rights and Welfare of the Child (Article 11), the African Union Principles on Freedom and Expression (Article 4), the American Declaration of the Rights and Duties of Man (Article 5), the Arab Charter on Human Rights (Article 21), and the European Convention for the Protection of Human Rights and Fundamental Freedoms (Article 8). Specific instruments dealing with the protection of personal data include the United Nations Guidelines for the Regulation of Computerized Personal Data Files.

A.1 Overview

Concepts of **privacy** vary considerably across countries and cultures, including in areas not related to identification (ID). It is therefore useful to frame the concern as applied to personal data in terms of **data protection**. One commonly used set of data protection principles is Fair Information Practices (FIPs) (Gellman 2016). The international policy convergence around FIPs is broad and deep, and the agreement has remained substantially consistent for several decades (Bennett 1992). FIPs originated in the 1970s with a report from a predecessor of the U.S. Department of Health and Human Services (U.S. DHEW 1973). A few years later, the Organisation for Economic Co-operation and Development (OECD) revised the original FIPs statement (OECD 1980); this became the most influential statement of the principles and is discussed further below.

Information privacy law and policy in many countries rely on FIPs for their core principles, including the European Union's (EU's) data protection directive (EU 1995) and many national laws in EU member states such as Canada,[1] as well as the Asia-Pacific Economic Cooperation's Privacy Framework (APEC Secretariat 2005).

1 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5), http://laws-lois.justice.gc.ca/eng/acts/P-8.6/; accessed December 2016.

In general, FIPs address data collection and purpose, data security, an individual's access to his or her own personal data, and the accountability of those managing the data. They can be formulated in a variety of ways, but the content of the different versions is substantially the same. The principles set out by the OECD (1980) are briefly described below.[2]

1. **Collection limitation principle.** There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and—where appropriate—with the knowledge or consent of the data subject.

2. **Data quality principle.** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

3. **Purpose specification principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection, and their subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use limitation principle.** Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the purpose specification principle except with the consent of the data subject or by authority of law.

5. **Security safeguards principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

6. **Openness principle.** There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual participation principle.** An individual should have the right (a) to obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him or her; (b) to have data relating to him or her

2 This text has been slightly modified from the original for style.

communicated within a reasonable time at a cost (if any) that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him or her; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied and to be able to challenge such denial; and (d) to challenge data relating to him or her and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

8. **Accountability principle.** A data controller should be accountable for complying with measures that give effect to the principles stated above.

A.2 Using FIPs to Develop Laws, Policies, and Best Practices

The FIPs elements provide standards for designing, operating, and evaluating the information privacy features of any information system. They reflect the basic premise that the best means of protection is simply to limit (1) the amount of information that is collected in the first place, and (2) access to such information. The greatest threat to the integrity of an information system may arise not from external hackers, but from people within the system—those who have been trusted with access, including government agencies and persons or organizations registered under the scheme—in accessing personal data.

A.2.1 Collection Limitation Principle

Limiting the collection of personal data is important, because the collection and maintenance of personal data elements may be unnecessary, may increase costs, may affect the rights and interests of data subjects in known and unforeseen ways, and is likely to result in greater pressure to use the data for secondary purposes. Data that are not collected do not become part of a central file on individuals, need not be protected against misuse, will not become a target for criminals seeking to engage in identity theft, and will not attract secondary users. ID schemes need to incorporate privacy protections, recognizing that even apparently innocuous-seeming information may have major security and privacy dimensions.

- **Collect only what is necessary for the purpose.** An effective way of promoting good privacy practice is to collect only the minimum amount of personal information that is necessary to meet a clearly defined and articulated purpose. Each data element collected should be evaluated and debated. The casual inclusion of information that might be useful someday should be resisted.

Collecting the minimal amount of data does the most to protect privacy. A biometric ID system might be able to function with only a name and one or more biometrics; gender and date of birth might be important, depending on the intended uses for the identifier.

- **Collect information by fair and lawful means.** An example of unfair data collection would be telling data subjects that the system collects facial photographs, but not informing them that the system secretly collects iris scans as well.

- **Exercise special care regarding sensitive data.** The United Nations characterizes the types of information that ordinarily should not be compiled as "data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, color, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union" (UN 1990, Principle 5).

  Other types of information can be sensitive in particular circumstances as well. People in certain professions, such as social workers, judges, and police officers, as well as refugees, may have concerns about the risk of threats being made to them or their families. Forms of harassment and stalking may create risks to safety. An individual's ability to apply for suppression of name and/or address information is a common resolution in such circumstances.

A.2.2 Data Quality Principle

The issue of what information needs to be retained and for how long should be considered in designing an ID scheme, including what happens to personal information when a person dies. Under internationally accepted privacy principles, information should be retained for no longer than necessary to fulfill the purpose for which it was originally obtained. The retention of photographs of the deceased may also raise cultural issues that need to be addressed.

Audit and verification processes are important mechanisms for ensuring data quality. In addition, schemes may include a requirement that places a degree of responsibility on individuals for notifying the administering authority, within a reasonable time period, if personal details (e.g., address or name) change. Such an obligation is commonly imposed under other government database programs internationally, especially those related to taxation and driver licensing. The nature of the data, and the potential

consequences of inaccuracy—e.g., blood type information—are also important factors that need to be considered.

The principle does not mandate the expenditure of resources to change records regularly unless the purpose of the systems requires that records be accurate, complete, or up to date. A record necessarily kept for an archival purpose would not need to be updated if the old record would not affect a current or future right, benefits, or privilege of the data subject. However, records stored for statistical purposes should not be retained in identifiable form. The EU data protection directive, for example, directs member states to establish appropriate safeguards for personal data stored for longer periods for historical, statistical, or scientific use (EU 1995, Article (6)(1)(e)).

A.2.3 Purpose Specification and Use Limitation Principles

The purpose specification principle works in tandem with the use limitation principle: specification of the purposes for any personal data processing implements the general policy that data collected for one purpose should not be used for another. Failure to follow this principle is what allows mission creep to occur. It may be unfair to ask an individual to provide personal information for any given activity and then to use that information for another purpose without either notice to, or the consent of, the individual. For example, it would be inappropriate to ask citizens to cooperate with a national census for the stated purpose of collecting statistical information for use on a nonidentifiable basis and then to allow the police to use individual responses to consider criminal charges against the citizens.

- **Rights of access to data must be clearly stated pursuant to law and be subject to oversight.** Specifically, enabling legislation should prescribe (1) what information may be disclosed, (2) to which agencies, (3) under what circumstances, and (4) the conditions of disclosure. Only those organizations explicitly authorized by legislation to access information should be able to do so. It should not be assumed, e.g., that private information will be available to the whole of government without restriction or limitation. The circumstances in which law enforcement authorities may access information—including any biometric components contained on the central database—also require careful consideration and regulation under any scheme.

- **Protections and limitations must be built in with regard to sharing personal information among government agencies.** Government agencies may wish to share such data for a range of reasons, including to provide better and more efficient services through coordinated delivery, to detect wrongdoing, and

to take joint action against social problems. However, it is important to build in protections and limitations to guard against the potential for abuse. The existence of an information-sharing program should be known and publicly justified in each case. Periodic reassessment is particularly valuable in helping to ensure that inroads to privacy would only be allowed where the benefits of sharing information continued to exceed the costs.

- **ID schemes can include controls aimed at defining the circumstances and operation of any data linking or computerized data matching.** Such controls can be accomplished through rules directed at (1) **authorization**—making sure that only programs clearly justified as being in the public interest are permitted to engage in data sharing or matching, (2) **operation**—ensuring that programs are operated consistent with FIPs, and/or (3) **evaluation**—subjecting programs to periodic review and possible cancellation.

- **Disclosure of information to nongovernmental entities must be carefully considered.** Where mechanisms are included that would make information available to nongovernmental entities, the following should be ensured: (1) strong privacy protections around the nature of the information disclosed; (2) clear regulation of the purposes for which information may be disclosed and how the information may be used; and (3) a robust accreditation mechanism to govern access to, and use of, such information. Relevant factors for determining disclosure include the following:

  - The proposed uses for, and the entity's lawful interest in, the information
  - The benefits to the public or any section of the public stemming from the user's handling of the register data
  - The benefits to the data subjects stemming from the user's handling of the register data
  - The risks to the lawful interests of the data subjects—in particular, to safety and privacy—that the user's handling of the register data presents or is likely to present
  - The adequacy, in light of the above, of the safeguards provided or to be provided by or on behalf of the user

  Conditions may be attached to accreditation of access to information that personal information obtained from a national register must not be manipulated, changed by scanning, resorted, or combined with personal information from any other registers. Such conditions can be focused on prohibiting data mining

that is unconnected with (1) the purpose for which the information was collected and disclosed, and (2) an identified public benefit. Where information is used for a nonpermitted purpose, or conditions of accreditation are otherwise breached, the sanction for an accredited user would be—at least—loss of accreditation status.

- **Identity should be reliably authenticated only where and to the extent necessary.** The degree of confidence with which an identity needs to be authenticated varies according to a number of risk factors, including the nature of the transaction and the value of that transaction. An individual should be able to know exactly who will be able to access what information and in what circumstances.

Implementing the purpose limitation and use limitation principles consistently and fairly can be challenging.

- **The purpose and use principles recognize several important exceptions.** Nothing in the purpose principle expressly prevents a broad statement of purpose, but any ID system runs the risk of becoming a general-purpose surveillance system in the absence of clearly defined limits.[3] Thus, an ID system that stated its purpose as determining both ID and program eligibility would not violate the principle by making eligibility determinations. Indeed, it would be possible in theory to define any lawful activity as a purpose. However, an overly broad or vague purpose statement would undermine rather than implement the principle. The EU data protection directive attempts to address this concern by stating that purposes must be explicit and legitimate (EU 1995, paragraph 28).

- **The principles recognize that it may not be possible or practical to specify in detail and in advance each purpose for which personal data are intended to be used.** For instance, any collection of personal data for ID may be subject to quality review by auditors or criminal review by police investigating misuse of the system by those in charge of system operations. These activities might not

3 An ID system can, consistent with the data quality principle, be used for a wide variety of ID activities. However, additionally using an ID system to determine program eligibility, to look for research subjects, or for other unrelated purposes would likely violate the purpose and use principles if those other purposes were not defined in advance. An example of a broader and questionable activity is the use of an ID system as a general-purpose surveillance system. If allowed, any ID system that maintains locations or transactions may allow police or other government agencies to track individuals—particularly if done without a lawful process such as a search warrant or other measures (e.g., high-level supervisory approval and/or for specific and limited purposes of compelling importance).

always be expressly identified in advance (Reidenberg et al. 2013). The purpose principle recognizes the problem by allowing use for other purposes that are **not incompatible** with the stated purposes. In this regard, the EU directive expressly states that secondary activities for historical, statistical, or scientific purposes are not considered incompatible with the purpose of any system (EU 1995, Article 6(1)(b)).

There are ways to impose controls on abuse of the incompatibility standards. Procedural controls may help, such as requiring appropriate supervisory approval, preventing individual staff members from making ad hoc determinations, notifying individuals of specific uses, or even requiring advance publication of any new not incompatible purposes. Advance legislative notice is also an option, as is public notice and comment on any determination regarding purposes determined to be not incompatible. Review or approval by a chief privacy officer (CPO; see below) or other data protection supervisory official may also provide some discipline.

- **The purpose principle allows uses with the consent of the data subject.** However, for many activities involving personal data and large numbers of data subjects, it will be impractical to rely on consent, and the administrative costs of managing consent can be high. It may be appropriate to use consent for some activities. An example is a research project looking at the uses of a biometric ID system in health activities. Such a project may also be appropriate for review by a human subject protection process, which may or may not include waivers of the need to obtain individual consent. Much would depend on national standards and existing policies for controlling research.

- **The principles allow use by authority of law.** A later statute can expand the purpose of an ID system and allow use of a biometric ID system for a new purpose not originally provided for by the statement of purpose. Later statutes can also be the cause of mission creep by expanding purposes far beyond the original plan.

A.2.4 Security Safeguards Principle

Recordkeepers bear a significant burden in protecting their data subjects from being the subject of criminal activity. Because security requirements vary over time and by technology, the principle goes no further than generalities. It has become a common practice to conduct a **risk analysis** (or **risk assessment)** of the appropriate security requirements for any complex information system (ISO 2013).

- Privacy requires personal information to be handled securely, whether while in storage, during transmission, or during use.

- Depending on what form the technology takes, security is needed in connection with any smart technology applications that may be implemented. In the case of a "smart" ID card, e.g., security considerations center on (1) can it be forged; (2) can information stored on the card be accessed, and if so, by whom; (3) can the card be remotely blocked if stolen; and (4) what other information can be accessed by the card.

- Many legislatures have enacted legislation mandating notice to data subjects about the loss or unauthorized acquisition of personal data (breach notification). The scope and standards of these laws vary. The cost of providing notice to data subjects can be great, and the consequences of a data breach are potentially disruptive and significant.[4] Some laws limit breach notification obligations when the underlying data are adequately encrypted. Even if there is no applicable legal requirement, any ID system might adopt breach notification as a matter of policy. Regardless, any database with personally identifiable information should have a policy and procedure addressing breach notification as well as plans for responding to an actual data breach.

A.2.5 Openness Principle

The openness principle requires that any data subject be able to learn of the existence of a processing operation, who is the data controller for that processing, and what personal data are being processed. A clear explanation of data policies—and the limits of those policies—should contribute to consumer acceptance of an ID system and diminish fears.

Particulars of the system should be available by means appropriate to the country in which the system operates—e.g., paper and/or Internet notices that each registered individual can receive/access and keep. Notices should include information that allows each data subject to exercise his or her rights to individual participation.

4 For a discussion and review of the cost of data breaches, see the Ponemon Institute's annual series of studies, http://www-03.ibm.com/security/data-breach/.

A.2.6 Individual Participation Principle

Each individual should have a right to know whether a data controller has data pertaining to him or her, a right to see and/or copy that data, a right to be given a reason if a request for access is denied and to challenge the denial, and a method to challenge and correct data that are not accurate or complete.

Any ID system must be prepared to address the problem of a compromised identifier. An individual should be able to obtain an adequate substitute for a compromised identifier.

A.2.7 Accountability Principle

There are many ways to provide accountability measures for FIPs. The principle for compliance with FIPs can be met with civil or criminal penalties, civil lawsuits, administrative enforcement, arbitration, internal or external audits, complaint processing, staff training, a privacy office or officer, and more. As an information system grows in importance, more measures may become appropriate. Some accountability measures focus on providing individuals with their rights under the law; some focus on institutional accountability. Obviously, accountability measures in any jurisdiction must reflect the local legal, administrative, and cultural norms.

- **Include fundamental protections in legislation rather than under regulations or rules.** While regulations and rules are attractive because they may be made quickly under delegated authority without submission to parliament, for these same reasons they also provide less certainty that important privacy and other protections will not be weakened or removed.

- **Legislation should provide for the establishment of any ID database that forms the basis of an ID system.** The discussion above highlights the nature of the protections, security protocols, access uses, usage restrictions, etc., that might govern the establishment, operation, and management of the database. (See the EU directive on the legal protection of databases; EU 1996.)

- **Enabling legislation should specify or establish the public agency that will have the mandate and responsibility to administer the scheme.** A source of funding will also need to be identified to ensure that this entity has the resources needed to carry out these additional functions. The question of ownership of

the underlying data, as well as any cards, should also be addressed by enabling legislation.[5]

- **The legal and regulatory enabling environment may include enforcement and compliance monitoring mechanisms that address the following:**
  - How the system will detect unauthorized access or misuse
  - What penalties will be imposed for unauthorized access or misuse
  - How the database will be kept secure especially from misuse, hackers, and unauthorized use and personnel
  - How individuals will be able to easily check their own data held in the database
  - What happens in the event of a data breach (data breach notification; see above)—what is the obligation of the database operator in notifying the data subject, including the timing and content of the notification as well as remedial measures
  - Who will monitor the system and whether the monitoring agency will be independent of government (including whether individuals will have the right to know who has accessed their data, when, and for what purpose)
  - How the system will ensure that data are accurate when they are entered for the first time, and what procedures will be in place to ensure that data are kept up to date and accurate
  - Right of redress in the event of unauthorized access, use, or disclosure of an individual's personal data
  - If applicable, the use of biometric features for ID purposes; in particular, the use of facial recognition and DNA raise acute privacy issues and should be dealt with in primary legislation

- **Development of a suite of measures providing strong, transparent oversight and governance is an important issue for further consideration.** Public accountability mechanisms comprise privacy protections supported by effective sanctions and remedies, as well as a clearly defined complaint-handling mechanism. Other oversight tools, such as powers of audit and investigation, should also be available to the relevant oversight body. Consideration can also

5 One approach is for each citizen to own any ID documents issued under a scheme and all associated personal data, enhancing individual sovereignty and potentially both enhancing privacy protection and limiting the scope for government to make decisions without an individual's knowledge or consent.

be given to permitting personal remedies for improper access and use by third parties.

- **Consider the appointment of a CPO.** A CPO is an official in a government agency, business, or organization responsible for managing the institution's privacy policy and its response to privacy laws. The CPO is a relatively new institution, arising in the last 15 years (Bamberger and Mulligan 2011). The 1990 German Federal Data Protection Law was the first to require an in-house data protection official for many nongovernmental companies and organizations (Korff 2010). CPOs are not the same as the privacy supervisory authorities established under the EU directive on data protection (EU 1995).

  A CPO functions at the organization level or, sometimes, at the program level. EU privacy supervisory authorities must operate with "complete independence" (Gellman 2016). In Germany, in-house data protection officials by law have a degree of independence from corporate management. Full independence for a CPO may not be possible, but the authority to report directly to the head of the agency operating the program, to the legislature, and to the public may be worth considering. A CPO with sufficient authority can be especially valuable in representing the interests of data subjects, identifying and limiting mission creep, reviewing security measures, and addressing data breaches.

Annex B. Institutional and Implementation Considerations

Implementing the introduction of a new or upgraded identification (ID) system at the national level or for a specific program requires significant resources and planning. It is typically a multiyear exercise likely to involve complex procurement, piloting and testing, capture of key information from individuals, creation and maintenance of a sophisticated data warehouse, delivery of physical ID cards and the development of processes and infrastructure that allow for a program or multiple programs to use the ID system for authentication. Legal considerations regarding privacy, data sharing, and security are also important elements; general principles are described in annex A.

B.1 Institutional Framework[1]

The institutional arrangements for foundational IDs vary across countries. One model, followed by a minority of countries including India, Pakistan, and Peru, is to implement the program through a specialized and autonomous technical agency. In most cases, ID agencies have emerged within ministries to serve other purposes such as determining citizenship or eligibility to vote. Depending on historical precedent, the provision of a national ID may be the responsibility of the ministry of interior, a body reporting to the ministry of justice, or an election commission. These arrangements can have implications for the incentives to promote universal registration and for collaboration with other parts of government, including in the administration of social programs.

Election bodies, for instance, are interested in the potential voter population, which is limited to adult citizens. The poor, for whom the transaction costs of enrolling to vote may be relatively high, may be excluded—especially if the costs of reaching them are high. The periodicity of elections will also affect incentives for updating data. Finally, the core mandate of election bodies, both functionally and legally, will be circumscribed to limit their interest or ability to work with other agencies.

There may be mechanisms put in place to facilitate better collaboration between existing ID agencies and other parts of government. It can be useful, e.g., to empower a coalition of government bodies when an identity system is extended. The Dominican Republic created a "social cabinet" to oversee the expansion of its national registration system to poor, unregistered citizens, though the Central Electoral Council played a

1 The information in this section is drawn from Gelb and Clark (2013).

lead implementing role. Mexico has a similar body, with representatives from various government stakeholders.

B.2 Procurement and Planning

B.2.1 Procurement

Procurement is an important step in developing or improving an ID system, since procurement decisions will greatly affect the system's success or failure and its cost. The key challenge for many governments is to ensure sufficient and up-to-date expertise regarding ID technology and services, as this is often not available within the responsible government entities. Procurement for ID systems can be divided into different areas:

- Plan and system specifications
- Information and awareness
- Enrollment (hardware, software and labor)
- Verification of captured data
- Deduplication
- Issuance of ID to enrolled individual (card manufacture and customization etc., mail or other delivery mode)
- Authentication (hardware, software, training etc.)
- Maintenance and updating of information
- Grievance/complaints/helplines

B.2.2 Determining Enrollment Approach

Regardless of whether enrollment is accomplished in a single countrywide push, is decentralized, or is handled through a gradual program, it is highly visible and the subject of intense focus. Honest assessment of a country's resources and infrastructure is critical in determining the appropriate approach to enrollment so as to best capture the on-the-ground reality. Key questions to ask in such an assessment

include the following; their consideration helps in identifying and addressing some of the key drivers of the ID enrollment process, software, and operational support.

- **How accessible are the various regions of the country?** The more difficult the access to regions, the more likely there will be populations not covered by the ID system. For an ID system to be inclusive and have a high level of coverage, it requires a proactive approach to enrollment. This proactive approach often includes enrollment teams traveling to remote areas and actively finding constituents. The inverse is also true, in that the more accessible the country, the easier it is to establish fixed enrollment centers in community areas.

- **Is there consistent power at enrollment locations?** Since ID systems are largely based around the collection of various digital data, power is important. If power is inconsistent or not available, a substitute needs to be provided—either battery power or a generator and petrol.

- **Is there a strong government infrastructure (buildings, support staff, etc.)?** It is important to understand the current state of the government infrastructure in the field. If there is a strong field-level government along with solid power and computing infrastructure, it is more likely the government can handle enrollment itself. If there is weak or limited infrastructure, it would be a good idea to use private sector partners in the actual enrollment. Use of such partners does not mean giving up control of the ID system, but instead having the private partners serve as the "feet on the ground" in the enrollment process. Note that certain constraints, such as a stable electricity source, will affect any attempt at enrollment, regardless of whether it is handled by the private or the public sector.

- **How much time does it take to enroll?** The length of time it takes in the field to do a standard enrollment will determine how many persons can be enrolled per computer per day. This information is critical for the enrollment team in allocating computer and other resources, as well as in determining building and infrastructure needs.

- **Are there cultural issues to be addressed?** It is important to take into account the need for male and female enrollment teams. This is especially complicated in mobile enrollment teams that have to travel to remote areas. Is there a scheduling option or is the enrollment on a first come, first served, basis? This can cause issues with both building and management, since a first come, first served, option requires a queuing and capacity management issue. You do not want a situation where you have one enrollment computer and 1,000

people show up to be enrolled. Language barriers can also be very important. Enrollment teams should be able to communicate in the local language. Equally important for mobile teams: how do they announce their activities and inform the population? What happens with persons that are absent on the days of enrollment in their community? How are the days set for enrollment activities (some days may be more or less suitable for making sure persons are available—market days, funeral days, etc.)?

- **What documents do individuals need to bring for enrollment?** This information is important not only in the actual enrollment process, but also in the communication plan, storage maintenance, and long-term operational management of the ID system. Also, in determining the documents to be provided, it is worth taking into account how easy or difficult it is to fake or forge them.

- **How does the enrollment team validate those documents?** The enrollment process needs to consider issues regarding fake or forged documents, and procedures need to be in place for agents to validate the requested documents.

- **How does the process ensure that the ID is received by the correct person?** The longer the lag between enrollment in the system and delivery of the ID, the more dramatic the potential impact on coverage. When IDs cannot be delivered at the time of enrollment, how will holders receive their IDs? And how will proper receipt be verified? It is commonplace to require people to return to the enrollment location to receive their IDs. This practice is problematic for the poor in many countries, as they have to take time off work, and it encourages rent-seeking by the holder.

B.2.3 Enrollment Centers

A significant factor in establishing a comprehensive national ID is the number of and distance between enrollment centers. The farther individuals have to travel and the longer they have to wait in line constitutes a financial burden, limiting the number of people who can afford to be enrolled. There are two methods that are often used to facilitate enrollment: **camp-based** enrollment in place for a short period of time and **static locations** that remain in place for long periods. The two options work very well in tandem, and are not as successful used independently.

In one low-income country, there was a massive enrollment, moving district to district in a camp-based scenario and staying at a single location for only two weeks at a time.

The initiative was perceived at the time as very comprehensive, but four years later, its success was shown to be limited, in that the exercise was not repeatable. Potential new registrants who had come of age in the intervening years could not travel to the capital to apply for an ID, thus creating a large population of unidentified residents. It was also found that a large number of the IDs issued had errors, but these could only be corrected by those who could afford to take time off work to travel to the capital. In addition, as the IDs begin to expire, they were not renewed because of the long travel times entailed.

Camp-style enrollments are highly effective in communicating the value and importance of an ID and how it will be used. The method also offers an excellent way to improve the ID system and enhance governmental reputation, since it can be used to confirm that people are receiving the promised benefits tied to their ID.

However, as the example outlined above shows, camp-style enrollments need to be supplemented. It is thus useful to have in place an extensive network of offices that are able to collect and update ID data. Post offices and schools are highly appropriate locations for ongoing enrollment and data correction, as people relate to them at a familiar, neighborhood level. In contrast, police stations—which are often associated with criminals and typically do not have a high level of trust within local markets—and election offices—which are often only staffed in the run-up to an election and thus do not constitute an ongoing ID service center—have been found to be very poor locations for this service.

B.3 Piloting and Testing

Since most of the technologies entailed in an ID system are by now quite stable and robust, piloting should focus on operational and implementation support structures within government and the private sector rather than on feasible use of biometric technology. And, because the collection of biometrics and the issuance of comprehensive national IDs is somewhat new for most countries, it is important to design and test business continuity strategies for when standard operating procedures break down. Some frequently overlooked continuity issues include the following:

- Crowd control
- Public information and awareness
- Power outages

- Delays in enrollment
- Complaint and feedback loops
- Incentives to obtain an ID (costs versus benefits)

When these issues arise, they can quickly put the quality and efficacy of the ID program at risk. In particular, it is important to provide complaint and feedback loops that can be tracked by the complainant and various civil society groups.

B.4 Database Maintenance and Security

A national ID system is about joining existing biographic information from the civil registry with biometrics to issue an ID to citizens and residents so as to authenticate the identity of the ID holder. It is the responsibility of the ID system and the issuing authority to ensure the safety and security of the enrollment data collected. The data captured (demographic and biometric) should be encrypted both at collection and transport. The ID authority should have a security policy in place, which will detail and define the security and access protocols to ensure data safety. The ID system must ensure the safety, security, and confidentiality of the data, to protect it from unauthorized access and misuse.

ID systems need to be treated with the highest level of security and recovery. These systems should be considered national assets, as they are the key to resident service delivery and government management. For this reason, proper support and operating costs must be ensured.

B.4.1 Data Center and Redundancy

Given the national importance of the data being collected and the high level of support, it is advised that at least a Tier 2 data center be used both for the primary and backup redundancy systems. This would include at least two copies of the entire system that can actively switch and scale based on demand and emergency management. The two data centers need to be located in different seismic zones, to limit the likelihood of both being affected by the same catastrophic event.

B.4.2 Security Framework

Special care needs to be taken to address the security of biometric information. Biometrics are unique to an individual and are therefore sensitive information that

needs to be protected with the highest standard of care to prevent any possibility of misuse. The biometric data should be encrypted immediately upon capture during the enrollment process. The data packet should be encrypted with a public and private key system and then securely transmitted to protect against unauthorized access and misuse.

Given the nature of the data and the likelihood of its malicious corruption or revision, all physical and digital access should be tracked by multiple sources. These systems need to be tested on a regular basis. Table B.1 presents a suggested minimum level of security that should be set for all system data, processes, and control requirements; these are detailed in the remainder of this section.

Table B.1 ID System Minimum Security Objectives and Recommendations

Control objective	Recommendation
Maintain an information security policy	Maintain a policy that addresses the various aspects of information security within the ID system; this should include the following: • Access requirements • Encryption standards • Emergency management
Maintain a vulnerability management program	• Use and regularly update antivirus software on all systems commonly affected by malware • Develop and maintain secure systems and applications
Implement strong access control measures	• Restrict access to resident data on a need-to-know basis • Assign and track all access to computers and data systems within the ID environment • Restrict physical access to all data
Build and maintain a secure network	• Install and maintain a firewall configuration to protect data • Implement an encryption standard for data both in transit and at rest • Do not use vendor-supplied defaults for system passwords and other security parameters
Regularly monitor and test network	• Track and monitor all access to network resources and resident data • Regularly test security systems and processes
Protect ID system data	• Limit access and track all access to system data • Encrypt transmission of ID system data across all networks, both public and private

B.4.2.1 Maintain an Information Security Policy

The issuing authority should create and maintain an information security policy that addresses the security requirements arising from functional/business needs and objectives. The objectives of this security policy are to

- provide management direction and support for information security;
- provide a baseline for information security;
- ensure appropriate safeguards and procedures are adopted to protect information and associated information technology resources;
- ensure that people handling information are aware of their accountability and responsibilities.

This policy should be implemented through a process approach based on "Plan, Do, Check, Act," as follows:

- **Plan.** Establish a security policy, objectives, targets, processes, and procedures relevant to managing risk and information security to deliver a high level of trust within the system.
- **Do.** Implement and operate the security policy, control processes, and procedures.
- **Check.** Monitor and review the security policy, control processes, and procedures.
- **Act.** Take corrective and preventive actions based on an audit and review to achieve continuous improvements to the security plan.

B.4.2.2 Maintain a Vulnerability Management Program

It is important to formulate risk assessment policies and procedures. To this end, all assets should be listed, threats and vulnerabilities identified and assessed, and a mitigation plan drawn up to be implemented for all threats. All vulnerable and high-risk components should be identified and protected. Specific recommendations follow.

- Use and regularly update antivirus software, anti-spyware, and other host protection systems on all systems commonly affected by malware.

- Develop and maintain secure systems and applications, including the adoption of a secure software development life cycle.

B.4.2.3 Implement Strong Access Control Measures

The issuing authority should identify all information assets and how they are used in the system. This should include the following actions:

- Restrict access to resident data by business need to know
- Assign a unique ID to each person with computer access
- Restrict physical access to resident data

Access control must take into account physical, host (computer), and network security.

B.4.2.4 Build and Maintain a Secure Network

It is essential that a secure network be established to protect the system from attack and misuse. Sample guidelines for securing the network include the following:

- **Install and maintain a firewall configuration to protect resident data.** A firewall is required to prevent external, potentially malicious, intruders from accessing the network and the resources within.
- **Do not use vendor-supplied defaults for system passwords and other security parameters.** A commonly ignored aspect of security is that various systems come with default security parameters, including passwords. The use of default settings may allow intruders to access the network and steal data/inflict damage.

B.4.2.5 Regularly Monitor and Test Network

Once a secure network is established, it must be regularly monitored, and steps must be taken to keep it up to date with regard to all security issues. Some possible mechanisms include the following:

- Track and monitor all access to network resources and resident data
- Regularly test security systems and processes

- Conduct regular security audits and penetration tests for all systems, networks, and processes to keep up to date with current threats and ensure against complacency

B.4.2.6 Protect ID System Data

The primary purpose of all security plans is to ensure that the resident data are not stolen, vandalized, or compromised in any way. To accomplish this, in addition to all the previous points, the registrar must classify resident data based on value and usage. Further, a cryptographic system must be put in place.

- **Encrypt resident data at rest.** All resident data must be encrypted while stored in external or internal secondary storage.
- **Encrypt resident data in motion.** All resident data must be encrypted when transmitted across open public—or even closed—networks.
- **Protect unencrypted data.** While the data are in the host memory, unencrypted, the host system must be protected from malicious activity, including viruses, spyware, etc.

B.4.3 Compliance

Compliance consists of three stages.

- **Collecting and storing.** Ensure secure collection and tamper-proof storage of all log data so that these are available for analysis.
- **Reporting.** Be able to prove compliance on the spot if audited and present evidence that controls are in place for protecting data.
- **Monitoring and alerting.** Have systems in place such as auto alerting, to help administrators constantly monitor access and usage of data. Administrators should be warned of problems immediately so they can rapidly address them. These systems should also extend to the log data—there must be proof that log data are being collected and stored.

Compliance can be accessed through the use of an annual onsite data security audit and quarterly network scans.

B.4.4 Data Structure

It is recommended that a single database not hold all of the data for a single user. It is advised that various pieces of data be assembled into a single structure only at the point the data are needed. This precaution limits the ability for a complete data compromise by forcing a would-be intruder to have to compromise several different systems to obtain a full record for an individual.

B.4.5 Encryption

Since ID system data are personal and are linked to other sensitive data, it is recommended that all data be encrypted, both while at rest as well as in transit. In-transit data should be encrypted with at least 128-bit encryption.

B.4.6 Additional Policies and Procedures

An ID system, as well as the various government and nongovernment actors involved with the system, should have the following in place:

- Information security and management policy
- Information security organizational structure policy
- Risk assessment policy and procedures
- Asset classification policy and procedures
- Asset classification and control standard
- Information labeling and handling procedures
- Acceptable use guidelines
- Procedures for control of documents and records
- Human resource security policy and procedures
- Physical and environmental security policy and procedures
- Change management policy and procedures

- Third-party management policy and procedures
- Antivirus and malicious software policy and procedures
- Backup and restoration policy and procedures
- Network security policy and procedures, including for Internet, intranet, mobile computing, teleworking, and firewall
- Media-handling policy and procedures
- Monitoring policy and procedures
- Access control policy and procedure (including password security)
- Network access control policy and procedures
- Systems development maintenance policy and procedures
- Incident management policy and procedures
- Business continuity management policy and procedures
- Cryptographic procedures document
- Minimum baseline security standards

B.5 Financing and Revenue

The cost of an ID program has historically been prohibitive, especially when including biometrics and authentication. Both the capital expense for initial enrollment and the cost of ongoing operational support of an ID system have been reduced in recent years. This reduction in cost is largely credited to India's ID system forcing a level of standardization and openness that the industry had resisted in the past; this system can serve as a baseline for cost comparison.

Comparing the costs of an ID system begins with delineating system components. As an example, in Rwanda's current ID system, it cost $18 million to issue 5.3 million IDs (Butera 2008). The main components of the Rwanda ID system are as follows:

- A polyvinyl chloride ID card (not a smartcard)
- Minimal manufacturing customization
- Demographic printing
- No personalization other than individual's photo
- Collects a fingerprint, signature, and digital photo
- No deduplication

The Indian ID system is significantly different, in that it does not issue a physical card but instead provides a 12-digit unique ID number that ties to the data within the system. Once completed, it is anticipated that the Indian ID system will cost $840 million for all of the country's 1.2 billion people. The important components of the Indian ID system are as follows:

- No ID card provided, just a printout of the number
- Digital capture of all 10 fingers, both irises, and a high-resolution photo
- Biometric deduplication
- Online verification of the ID number to biometrics

B.5.1 Biometrics

Historically, the collection of biometrics increased not only the cost of hardware but also operating cost, due to the time that was required to process enrollments. With the definition of open standards and the elimination of the proprietary nature of the hardware, costs have dramatically decreased. As of early 2013, the cost of a 10-fingerprint scanner appropriate for use in India's ID program had dropped from almost $4,000 to less than $1,000. Iris scanning equipment has similarly dropped in price, from over $7,000 to below $2,500. Moreover, the new devices that the Indian project has caused to enter the ecosystem are pushing these costs down further. Components of the enrollment kit for India's ID program are listed in table B.2.

Table B.2 India ID System Enrollment Kit Components

Component	Description
Laptop	Intel i3 processor 2.2 GHz, 4 GB RAM, 800 MHz FSB,2 MB L2 cache, 250 GB 5400 RPM SATA hard drive, USB 2.0 ports—4 Nos., preloaded OS: Microsoft Windows 7 Professional, antivirus—Microsoft Security Essential or Antivirus–Internet Security–Quick Heal
Additional TFT monitor	15.6" TFT Acer Monitor
Web camera	2 megapixel Logitech Pro 9000 series
Fingerprint scanner	Live scan capturing 10 fingerprints (4-4-2)
Iris scanner	Dual iris capturing
1 KVA offline UPS	Ibetex/APC
Pen drive	4GB Kingston
500 GB external hard drive	Samsung
Printer	Samsung Mono Laser Printer A4
Lighting	1 wide florescent lighting kit
Background screen	1 extra white without stand background screen
Uniform	1 t-shirt with ID program logo
	USB hub
	Extra-durable hard-side carrying case that fits all the above equipment

B.5.2 Deduplication

Deduplication was formerly cost prohibitive for most countries, both from a technological aspect and in terms of managerial ability. These systems were very complex and required significant amounts of computing resources, which meant vendors could lock a country into using only their systems. But the use of unique contracting relationships and standard technologies for the collection of biometrics has forced legacy vendors to drop their prices and open up their architecture, in addition to having new vendors provide solutions. In late 2006, the cost to deduplicate was as high as $0.80 per finger. As of late 2012, this price had dropped to below $0.06 per finger for countries with sufficient volume, or $0.10–$0.20 in other countries.

B.5.3 Authentication

Most ID systems have been limited to manual verification using a "best guess" comparison of the ID and the photo that is printed on the ID, or an expensive system with a biometric stored on a smartcard. The smartcard pushed the cost of the physical

card up significantly and required a substantial investment in card stock management procedures. With the advent of web-based technologies and extensive wireless networks, it is now possible to provide for ID and personal authentication via a stored biometric within the system. These systems are often sold in 100,000 authentications-per-day blocks and currently average about $80,000 per 100,000 per day. As an example, the hardware and software cost to support 500,000 biometric-based authentications per day from various users of the ID system (banks, subsidy delivery, health care, and mobile phone providers) would be $400,000.

B.5.4 Operational Costs

Historically, a country would have to pay a vendor a yearly licensing fee along with several different licenses for patents, but the systems discussed above do not require these ongoing licensing fees; and, in most cases, do not have any ongoing financial requirements other than support services that can be contracted on an as-needed basis.

B.5.5 Financing of ID Systems

Much work has been done in determining ways to finance these systems through the World Bank. Several projects around the globe have supported the building, implementation, and operational requirements of these ID systems because of the improvements they afford in service delivery throughout the government.

It is advisable for governments to seek independent technical support or ensure sufficient internal expertise for sound decision making, so as not to depend on the advice of vendors. This is critical because of the highly technical nature of these types of systems and the specialized contracting ability of various vendors.

B.5.6 Revenue Models

The authentication process can be used as a revenue generator to offset some of the costs of the system's ongoing management. In most cases, this is a cost that is passed on to organizations, such as banks or mobile phone providers, requesting authentication of a user or an ID from the system. These authentication service fees frequently range from $0.05 to $0.10, depending on the type and number of authentications. In one Asian country, this service fee generated sufficient funding to pay for the ID system in full in less than five years. The funding also helped improve the quality and stability of the issuing authority, as it did not require ongoing budgetary support from the general treasury.

Bibliography

APEC (Asia-Pacific Economic Cooperation) Secretariat. 2005. *APEC Privacy Framework*. Singapore: APEC Secretariat.

Bamberger, Kenneth A., and Deirdre K. Mulligan. 2011. "New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States." UC Berkeley Public Law Research Paper No. 1701087. University of California Berkeley.

Barnwal, Prabhat. 2015. "Curbing Leakage in Public Programs with Biometric Identification Systems: Evidence from India's Fuel Subsidies." Paper. School of International and Public Affairs, Columbia University, New York.

Bennett, Colin J. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University Press.

Butera, Saul. 2008. "Rwanda: National ID Distribution Resumes." *The New Times* October 9.

EFF (Electronic Frontier Foundation). n.d. "Mandatory National IDs and Biometric Databases." Website.

EU (European Union). 1995. "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data."

——. 1996. "Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases."

Fenker, Samuel P., and Kevin Bowyer. 2012. "Analysis of Template Aging in Iris Biometrics." In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*.

Fussell, Jim. 2001. "Group Classification on National ID Cards as a Factor in Genocide and Ethnic Cleansing." Presentation. Prevent Genocide International.

Gelb, Alan, and Julia Clark. 2013. *Identification for Development: The Biometrics Revolution*. Washington, DC: Center for Global Development.

Gellman, Robert. 2016. "Fair Information Practices: A Basic History." Version 2.16.

Harbitz, Mia, and Bettina Boekle-Giuffrida. 2009. "Democratic Governance, Citizenship, and Legal Identity: Linking Theoretical Discussion and Operational Reality." Working paper. Inter-American Development Bank, Washington, DC.

Hu, M. 2013. "Biometric ID Cyber Surveillance." *Indiana Law Journal* 88: 1475–1558.

IDB (Inter-American Development Bank). 2011. "Uruguay Strengthens Civil Registry." Webstory September 19.

ISO (International Organization for Standardization). 2013. "Introduction to ISO 27002 (ISO27002)."

Korff, Douwe. 2010. "New Challenges to Data Protection: Country Study A.4 – Germany." European Commission, Directorate-General Justice, Freedom and Security.

OECD (Organisation for Economic Co-operation and Development). 1980. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."

OHCHR (Office of the High Commissioner for Human Rights). 2012. *Guiding Principles on Extreme Poverty and Human Rights*. Geneva: OHCHR.

Reidenberg, Joel R., Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu. 2013. *Privacy and Missing Persons after Natural Disasters*. Washington, DC, and New York: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars.

Reuben, William, and Ricardo Cuenca. 2009. "El estado de la indocumentacion infantil en el Peru: Hallazgos y propuestas de politica." Working paper. World Bank, Washington, DC.

UN (United Nations). 1990. "Guidelines for the Regulation of Computerized Personal Data Files." General Assembly Resolution 45/95.

UNICEF (United Nations Children's Fund). 2012. *Children in an Urban World: The State of the World's Children 2012*. New York: UNICEF.

U.S. DHEW (U.S. Department of Health, Education & Welfare). 1973. "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems." DHEW Publication No. (OS) 73-94. Washington, DC: DHEW.

World Bank. 2007. "Project Appraisal Document on a Proposed Loan in the Amount of US$19.4 Million to the Dominican Republic for a Social Protection investment Project." World Bank, Washington, DC.

ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

QUESTIONNAIRE

DELIVERY

The following is a simplified version of the full Identification Systems for Social Protection questionnaire, available for download in Excel format at ISPATools.org.

Contents

1: Background Information and Scope of the Assessment Q-4
1.1 Context of the Assessment Q-4
1.2 Scope of the Assessment Q-4
1.3 Country Background Information Q-4
1.4 Country Background Social Protection Information Q-4
2: Civil Registration and Identification Ecosystem Q-5
2.1 Civil Registration and Vital Statistics Q-5
2.2 Overview of the National ID Q-8
2.3 Description of the National ID Document and Number Q-8
2.4 Issuing Agency Q-9
2.5 Enrollment and Issuing Process Q-10
2.6 Data and Deduplication Q-11
2.7 Uses of the National ID Q-12
2.8 Other ID Systems Existing at National Level Q-13
2.9 Personal Data Protection Q-15
3: Introduction to the Assessed ID System Q-16
Criterion A: Coverage and Accessibility Q-17
A.1 Coverage of the ID System Q-17
A.2 Ease of the Enrollment Process Q-18
A.3 Transaction Cost to Enroll in the ID System Q-18
A.4 Inclusiveness Q-19
Criterion B: Robustness of the System and Its Information Q-20
B.1 Uniqueness Q-20
B.2 Credential and Data Security Q-20
B.3 Authentication Procedure Q-21
B.4 Database Management (update) Q-22
Criterion C: Costs Q-23
C.1 Infrastructure Q-23
C.2 Maintenance Q-23
C.3 Other Q-23

Criterion D: Coherence, Interoperability, and Integration Q-24
D.1 Coherence Q-24
D.2 Interoperability and Regulations Related to the Exchange of Information Q-24
D.3 Ubiquity/Portability Q-25
Criterion E: Governance and Respect of Rights and Dignity Q-25
E.1 Governance Framework Q-25
E.2 Institutional Capacity Q-26
E.3 Respect for Rights and Dignity Q-26

1: Background Information and Scope of the Assessment

1.1 Context of the Assessment

1. Name of the country
2. National organization leading the assessment
3. Associated experts (name, position, organization)
4. Start date of the assessment
5. Interviewed/consulted organization
6. Objective(s) of the assessment:
    a. Improvement of a given ID system used for social protection
    b. Identification of the best ID system for a new social protection program
    c. Rationalization of existing ID systems in the field of social protection
    d. Contribution to the definition of an ID strategy for social protection
    e. Other, please specify

1.2 Scope of the Assessment

7. Please list the different ID systems (foundational and functional) that will be assessed.

1.3 Country Background Information

8. Income level
9. Number of inhabitants (nationals and non-nationals)
10. Share of rural population
11. Institutional delivery rate
12. Birth registration rate (i.e., issued birth certificate)
13. Death registration rate
14. Number of existing ID systems

1.4 Country Background Social Protection Information

15. List the main social protection programs existing in the country.

Program name	Program type/ benefit provided	Objective	Managing institution	Annual coverage	Annual budget	Used ID system

2: Civil Registration and Identification Ecosystem

1. Is there a national strategy for identification? Yes/no
2. If yes, which of the following are objectives of this strategy?
   a. Reduce coverage gaps
   b. An integrated national identification system
   c. Establish a unified system of civil registration and identification
   d. Reduce leakages in social protection programs
   e. Reduce exclusion from social protection programs
   f. Ensure identification for know your customer (KYC) for financial inclusion
   g. Security and border control
   h. Other, specify
3. Is there a coordination body or steering committee involving different government agencies and stakeholders that focuses on improving coordination of identification across sectors and programs? Yes/no
4. Is there a national strategy for communication and awareness for the national-level ID? Yes/no
5. What approach or approaches are taken for extending awareness?
   a. Periodic information campaigns at local level
   b. Permanent process of advertisement and dissemination
   c. Linking ID to specific incentives
   d. Customizing awareness campaign to specific groups (e.g., indigenous)
   e. Other, specify

2.1 Civil Registration and Vital Statistics

6. Is there national legislation that makes the registration of births and deaths mandatory? Yes/no

7. What government entity is responsible for administering the civil registration system?
    a. Ministry of interior
    b. National ID agency
    c. Specialized, autonomous agency (name)
    d. Other, please specify
8. Does the responsible agency have formal cooperation arrangements with other agencies or organizations to improve inclusion and access to registration and identification documents?
    a. Yes, with other government agencies
    b. Yes, with the private sector
    c. Yes, with international agencies and donors
    d. Yes, with nongovernmental organizations
    e. Yes, with other organizations, please specify
    f. No
9. Are there budgetary incentives in place based on results in terms of the coverage of civil registration and identification? Yes/no
10. Are birth and death registrations digitized, stored electronically? Yes/no
11. Are those registered as dead removed or deactivated from the national ID database? Yes/no
12. What is the total number of offices that handle civil registry functions across the country including the decentralized or local offices?
13. What percentage of these offices are estimated to have the following infrastructure capacity?
    a. Photocopiers
    b. Telephone
    c. Computers
    d. Electronic forms
    e. Capacity to transmit data by Internet
14. What is the process from birth to the issuance of birth certificate (what actions, completed by whom)?
15. How long is the process from the time of birth to the issuance of a birth certificate (number of days)?

16. Are there specific population groups that encounter obstacles to obtaining a birth certificate?
    a. Yes, indigenous people
    b. Yes, migrants and/or nomadic people
    c. Poor people
    d. Women
    e. Other, please specify
17. What is the process to register death (what actions, completed by whom)?
18. What is the estimated percentage of births that take place in medical facilities (i.e., institutional births)?
19. What is the estimated percentage of actual births that are registered (i.e., issued birth certificates)?
20. Are there regulations or norms that oblige hospitals and clinics to report births and deaths to the civil registration authority in a prespecified period of time? Yes/no
21. Is there a mechanism for working with communities and community leaders for registration of non-institutional births? Yes/no
22. Is birth registration information centralized at the national level? Yes/no
23. How is documentation about births and deaths from local and regional offices transferred to a central, national data repository?
    a. Online transfer in real time
    b. Electronic transfer periodically
    c. Physical files or copies periodically transferred
    d. Documentation is not transferred and remains at the local agency
24. Is there a specified time frame for this transfer to occur?
    a. n/a
    b. No
    c. Yes, the time frame is:
25. What is the process to get birth and death certificates (what actions, completed by whom)?
26. How long does it typically take to obtain a birth certificate?
27. Can individuals request birth and death certificates in any civil registry office in the country independent of where the original registration took place? Yes/no
28. Are there mobile units or kiosks that allow individuals to obtain these certificates without having to visit civil registry offices? Yes/no

29. How much does it cost for an individual to obtain a birth certificate at a civil registry office?
30. What is the annual budget for civil registration (latest year available)?

2.2 Overview of the National ID

31. Does a nationally issued ID exist? Yes/no (If no, skip this subsection)
32. What is the title of the legislation that establishes and defines this form of identification and the year that it was approved?
33. Is the national ID intended to cover
    a. All residents
    b. All citizens
    c. All adult citizens or voters
    d. Other, please specify
34. How is the national-level ID system linked to birth and death registries?
    a. It is not
    b. Births and deaths are reported to the agency intermittently and updated
    c. Birth registration is regularly communicated to the ID agency
    d. Death registration is regularly communicated to the ID agency
    e. Birth registration is directly linked to the issuance of a new national-level ID
35. When was this ID, in its current form, first issued?
36. How many IDs were issued last year?
37. How many IDs have been issued to date (cumulative figure)?
38. What proportion of these are deduplicated?
39. How many IDs are estimated to be held by individuals today (IDs issued net of deceased ID holders)?
40. What is the estimated number of undocumented or illegal residents or noncitizen refugees?

2.3 Description of the National ID Document and Number

41. What kind of ID document is issued?
    a. None
    b. Paper
    c. Bar code

d. Magstripe
e. Smart card

42. What information is printed on the ID document?
    a. ID number
    b. Name
    c. Address
    d. Age
    e. Sex
    f. Ethnicity
    g. Political affiliation
    h. Religion
    i. Other, specify
43. What information is stored on the card that is not visible but machine-readable (if any)?
    a. ID number
    b. Name
    c. Address
    d. Age
    e. Sex
    f. Ethnicity
    g. Political affiliation
    h. Religion
    i. Biometrics
    j. Other, specify
44. How many digits are in the ID number?
45. Is there logic in the number? Yes/no

2.4 Issuing Agency

46. What is the name of the agency that is responsible for issuing this ID?
47. Is this an independent agency (i.e., not part of another agency or ministry)?
48. If no, to what ministry or other government entity does it report?
49. What is the annual budget of this entity?

50. How many branch offices does it have?
51. How many employees/staff?

2.5 Enrollment and Issuing Process

52. What is the process to get a national ID (what actions, completed by whom, and where)?
53. What is the age requirement for obtaining this ID?
    a. None
    b. Voting age
    c. Age considered as an adult
    d. Other, specify
54. What documents are required to apply for this ID?
    a. None, issued at birth along with birth certificate
    b. Birth certificate
    c. Community verification/affidavit
    d. Verification of another individual or individuals
    e. Other
55. What is the estimated number of days that it takes to issue a new ID document in the following cases:
    a. New ID
    b. Renewal
    c. Lost or stolen
    d. Other, specify
56. How often must the ID be replaced?
    a. Never
    b. Less than every five years
    c. More than every five years
57. How much does the ID cost to be produced and issued?
58. What is the official cost for the people to obtain the document? What is the real cost reported to be?
59. Is there a specific fee for replacing a lost or stolen ID? If yes, how much?
60. In the case of an individual who does not have a birth certificate but wishes to apply for a national ID, what is the process?

a. There is no process defined or in place
b. Individual must obtain a birth certificate first by documenting his/her identity through multiple witnesses with notarization or some other legal certification process
c. Individual must obtain birth certificate first documenting his/her identity through witnesses recognized by the national ID agency without further legal process
d. Individuals can obtain both the birth certificate and national ID through the same enrollment process using witnesses
e. Other, please specify

61. Are there particular categories of the population that face geographic, cultural, economic, or legal barriers that prevent them from obtaining this ID? Please specify the type of barrier.
    a. Yes, migrants
    b. Yes, indigenous people
    c. Yes, women
    d. Yes, other groups, specify
    e. No
62. Are there specific policies to address the most vulnerable population groups? Yes/no If yes, please describe the policies
63. Do responsible agencies provide free services for vulnerable groups of the population? Yes/no
64. If yes, how are these groups designated (e.g., targeting mechanism or other criteria)?

2.6 Data and Deduplication

65. What information is captured in the ID database for those enrolled?
    a. Name
    b. Date of birth
    c. Sex
    d. Address
    e. Ethnicity
    f. Religion
    g. Political affiliation

h. Information on parents or other family members
i. Other, please specify

66. Is a photo captured at the time of enrollment?
    a. Yes
    b. No
    c. Other
67. What other biometric information, if any, is captured at enrollment?
    a. None
    b. Fingerprints
    c. Iris
    d. Digital facial image
    e. Other, please specify
68. What is the deduplication strategy if any?
69. Are biometrics used to ensure that new ID numbers are not issued for people already in the database (i.e., deduplication)? Yes/no
70. Is there a mechanism for changing information on the ID? Yes/no
71. How many requests for such changes are processed annually?

2.7 Uses of the National ID

72. Is the national-level ID used commonly for any of the following purposes?
    a. Opening a bank account
    b. Obtaining credit or loans
    c. Reporting to the tax authority
    d. Obtaining marriage certificate
    e. Obtaining private health insurance
    f. Enrolling in social insurance programs
    g. Qualifying for cash transfers, food, or other safety net programs
    h. Getting a cell phone account
    i. Obtaining a passport
    j. Getting a driver's license
    k. Voting
    l. Registering a vehicle

m. Purchasing property
n. Other, specify

73. In which of these databases would the national, personal identification number be included?
    a. Social insurance programs
    b. Social assistance programs
    c. Income tax records
    d. Vehicle registration
    e. Driver's license
    f. Voter registration rolls
    g. Credit rating agency records
    h. Bank records
    i. Utility billing records
    j. Criminal records
    k. Passport records
    l. Formal employment records
    m. Private insurance records
    n. Other, specify
74. Does the ID agency use IDs to help other government entities to cross-check databases? Yes/no
75. If yes, what kind of cross-checking is done?
    a. Social insurance and social assistance
    b. Social assistance and income tax data
    c. Social insurance and income tax data
    d. Property/assets and income tax data
    e. Public employment status
    f. Other, specify

2.8 Other ID Systems Existing at National Level

76. How many government agencies issue their own forms of ID cards?
    a. 1
    b. 2

c. 3–5

d. 6–10

e. 10+

77. Please specify all different ID systems existing at the national level and indicate which one is the most prevalent.

	Short description	Issuing agency	Link with the national ID	Link with civil registry	Coverage
Tax identifier					
Voter ID					
Social security #					
...					

78. Are there formal coordination mechanisms between government ID card issuers? Yes/no

79. Are there standards for data formats and fields that apply across the major government databases?

a. Yes, but only for a subset of government agencies/programs

b. Yes, and widely applied

c. No

80. Are there common ID authentication standards for transactions in different programs?

a. Yes, for most transactions there is a single authentication mechanism

b. Yes, for some transactions there is single authentication mechanism

c. No

81. How many of the major government programs require some form of electronic authentication using these IDs?

a. 1

b. 2

c. 3

d. 4

e. 5 or more

82. How many government programs require biometric verification of identity using this ID in order to receive a benefit?

a. 1

b. 2

c. 3
d. 4
e. 5 or more

83. Are there any private transactions that use this ID to electronically verify identity at the point of the transaction? Yes/no

2.9 Personal Data Protection

84. Are there explicit rules and regulations as to how government agencies can link their databases using the national ID? Yes/no
85. Is there an explicit list of government agencies that are allowed to access the national-level ID database? Yes/no
86. Is there a standard format for memorandums of understanding (MOUs) between the ID issuing agency and other government agencies? Yes/no
87. Is there legislation on privacy or protection of personal data that delimits the access and use of data in the national ID database? Yes/no
88. Has a privacy impact assessment ever been conducted? Yes/no
89. Does the legislation establishing the national-level ID clearly establish protection of privacy of data? Yes/no
90. If yes, are there ambiguities or broad exceptions to this protection that could be abused? Yes/no
91. Is the public reporting of exceptional cases of accessing data (e.g., based on national security threats) required? Yes/no
92. Is there a supervisory body within government responsible for monitoring compliance with privacy and data protection rules? Yes/no
93. Are the penalties for violation of the privacy rules clearly established and appropriate? Yes/no
94. Is the process for grievance redress for individuals who claim their privacy was violated clear? Yes/no
95. Is the information that must be provided for obtaining the national-level ID the minimum required for the purposes of this ID? Yes/no
96. How are data encrypted (when at rest/when in motion)?
97. Is all access to computers and data systems within the ID environment assigned and tracked?
98. Are security systems and processes regularly tested?

99. What other measures are taken to ensure networks, systems, and applications are secure?
100. Which of the following procedures or policies are in place?
    a. Information security and management policy
    b. Information security organization structure policy
    c. Risk assessment policy and procedures
    d. Asset classification policy and procedure
    e. Asset classification and control standard
    f. Information labeling and handling procedure
    g. Acceptable use guideline
    h. Procedure for control of documents and records
    i. Human resources security policy and procedure
    j. Physical and environmental security policy and procedure
    k. Change management policy and procedure
    l. Third-party management policy and procedure
    m. Antivirus and malicious software policy and procedure
    n. Backup and restore policy and procedure
    o. Network security policy and procedure (including Internet, intranet, mobile computing, teleworking, firewall security)
    p. Media-handling policy and procedure
    q. Monitoring policy and procedure
    r. Access control policy and procedure (including password security)
    s. Network access control policy and procedure
    t. Systems development maintenance policy and procedure
    u. Incident management policy and procedure
    v. Business continuity management policy and procedure
    w. Cryptographic procedure document
    x. Minimum baseline security standards

3: Introduction to the Assessed ID System

These and the other sheets in Module three of the questionnaire need to be filled in for each functional ID system included in the assessment.

1. What is the name of the ID system?
2. What organization is responsible for this ID?
3. When was the ID system created?
4. When was the current form of this ID first issued?
5. Is it an individual or a household ID system?
6. What is the history of its creation?
7. List the main social protection programs using this ID system, if any:

Program name	Program type	Objective	Managing institution	Annual coverage	# of beneficiaries	Benefit provided	Annual budget

8. What is the age requirement for obtaining this ID, if any?
   a. None
   b. Voting age
   c. Age considered as an adult
   d. Other, specify
9. What is the legal framework of this ID system, if any?
10. Insert a picture of the ID card, front and back.
11. How many individual IDs were issued cumulatively?

Criterion A: Coverage and Accessibility

A.1 Coverage of the ID System

1. Describe the intended covered population.
2. How many individuals does this represent?
3. How many individual IDs were issued during the last year?
4. How many individual IDs have been issued cumulatively?
5. How many IDs are estimated to be held by individuals today (valid IDs issued net of deceased ID holders)?
6. What share of the targeted population is covered?
7. How many individuals does this represent?
8. What approach or approaches are taken for extending awareness?
   a. Periodic information campaigns at local level

b. Permanent process of advertisement and dissemination
c. Linking ID to specific incentives
d. Customizing awareness campaign to specific groups (e.g., indigenous)
e. Other, specify

A.2 Ease of the Enrollment Process

9. What is the name of the agency that is responsible for issuing this ID?
10. At what layer of the administration is this agency working?
11. What is the enrollment strategy (active/passive)?
12. What is the process to get an ID (what actions, completed by whom, and where)?
13. What documents are required to apply for this ID?
    a. National ID
    b. Birth certificate
    c. Community verification/affidavit
    d. Verification of another individual or individuals
    e. Other
14. How long is the application form to request the ID?
15. Is any support provided to fill out the form?
16. How long does it take to receive the ID?
17. Who is in charge of delivering the ID to individuals, and how is this done?
18. How often must the ID be replaced?
    a. Never
    b. Less than every 5 years
    c. More than every 5 years
19. Are there mobile units to complete the enrollment process?
20. Are the open hours of the office compatible with the living schedule of the targeted population?

A.3 Transaction Cost to Enroll in the ID System

21. How far from the living areas are registration facilities located?
22. What would be the average cost for an individual to go there?
23. How long does it takes to complete the enrollment process?

24. How long do individuals have to queue before starting their enrollment process?
25. How much is the individual enrolled charged for this ID?
    a. Nothing
    b. $1
    c. $1–$3
    d. $3+
26. Is there any other related expense for the individual?
    a. Identity photos
    b. Certificates gathered in other administrations
    c. Photocopies
    d. Other, please specify
27. Is there any case of corruption reported?
28. Is there a cost to the individual for replacing a lost or stolen ID?

A.4 Inclusiveness

29. What barriers to enrollment have been identified by the responsible agency (ies)?
    a. Economic
    b. Geographic
    c. Cultural
    d. Legal
    e. Religious
    f. Other, specify
30. Are there particular categories of the population that face geographic, cultural, economic, or legal barriers that prevent them from obtaining this ID? Please specify the type of barrier.
    a. Yes, migrants
    b. Yes, indigenous people
    c. Yes, women
    d. Yes, other groups, specify
    e. No
31. Are there specific policies to address the most vulnerable population groups?
32. Is there a mechanism for timely registration of newborns in the ID system?

33. In case an individual cannot produce all requested documents, is there any derogation to the enrollment process?

Criterion B: Robustness of the System and Its Information

B.1 Uniqueness

1. How is uniqueness ensured (i.e., that each person can only be entered once into the database)?
2. Is the ID database deduplicated?
3. If yes, what is the deduplication strategy?
4. Are biometrics used to deduplicate? Yes/no
5. Is there logic in the number? Yes/no
6. How is the uniqueness of the ID number ensured?

B.2 Credential and Data Security

7. What kind of ID card is issued?
    a. None (no card issued)
    b. Standard (e.g., paper, photo ID)
    c. Bar card
    d. Magstripe
    e. Smart card
8. What information is printed on the face of the card?
    a. ID number
    b. Name
    c. Address
    d. Age
    e. Sex
    f. Ethnicity
    g. Political affiliation
    h. Religion
    i. Other, specify

9. What information can be derived from the card that is not visible but machine-readable?
    a. ID number
    b. Name
    c. Address
    d. Age
    e. Sex
    f. Ethnicity
    g. Political affiliation
    h. Religion
    i. Biometrics
    j. Other, specify
10. What security features (aside from smart encryption) are on the card?
    a. Holograms
    b. Micro printing
    c. UV printing
    d. Laser engraving
    e. Tactile
    f. Other, specify
11. Have there been attempts to access program benefits using false IDs? Yes/no
12. If yes, does this happen:
    a. Frequently
    b. Infrequently
    c. Rarely

B.3 Authentication Procedure

13. Describe the authentication procedure.
14. Is the ID used for authentication at the point of benefit delivery? Yes/no
15. If yes, which form of authentication is used:
    a. Biometric, off-line verification
    b. Biometric, online verification
    c. PIN-based, off-line verification

d. PIN-based, online verification
e. Photo
f. Match with other form of ID (e.g., national ID number)
g. Other, please specify

16. Are there transactions where the biometrics on the card, if any, are used to verify identity/authenticate? Yes/no

B.4 Database Management (update)

17. What information is captured in the ID database for those enrolled?
    a. Name
    b. Date of birth
    c. Sex
    d. Address
    e. Ethnicity
    f. Religion
    g. Political affiliation
    h. Information on parents or other family members
    i. Socioeconomic variables (income, housing type, etc.)
18. Is a photo saved in the database? Yes/no
19. What biometric information, if any, is in the database?
    a. None
    b. Fingerprints
    c. Iris
    d. Digital facial image
    e. Other, please specify
20. Is information stored using standard data formats and fields that apply across the major government databases?
    a. Yes, but only for a subset of the data
    b. Yes, and widely applied
    c. No
21. Is there a mechanism for changing information on the ID database? Yes/no
22. How many requests for such changes are processed annually?

23. Are there clear rules for access to the data maintained by the program? Yes/no
24. Are the IDs of those registered as dead removed or deactivated? Yes/no

Criterion C: Costs

C.1 Infrastructure

1. If an ID card is issued, what is the unit price of producing the card?
2. What is the unit price of a card printer?
3. How many card printers were purchased?
4. What is the unit price of a card reader?
5. How many card readers were purchased?
6. What was the cost of the information technology (IT) infrastructure to maintain the database?

C.2 Maintenance

7. How many staff are needed to administer the system (registration, authentication, database management, and administration)?
8. What is the staff cost?
9. What is the expected life span of the ID system/hardware/ID card?
10. How much is spent on other recurrent costs (Internet, electricity, etc.)?

C.3 Other

11. How much was spent on training staff on operating the ID system?
12. How much was spent on backup solutions for alternative identification solutions if the primary system fails?
13. Other costs?
14. What is the cost of the ID system compared to total program expenditure/total administrative costs?

Criterion D: Coherence, Interoperability, and Integration

D.1 Coherence

1. Is the national ID card required to register in the database? Yes/no
2. If yes, what proportion of beneficiaries have national ID numbers in the database?
3. Is there any other ID that is registered in the database?
    a. Voter ID
    b. Birth certificate ID
    c. Social security ID
    d. Other, please specify

D.2 Interoperability and Regulations Related to the Exchange of Information

4. How is the ID database linked to birth and death registries?
    a. It is not
    b. Births and deaths are reported to the agency intermittently and updated
    c. Birth registration is regularly communicated to the ID agency
    d. Death registration is regularly communicated to the ID agency
5. How is the ID database linked to the national ID database?
    a. It is not
    b. The national ID database is used for deduplication
    c. The national ID card is in the database but there is no secure electronic link between the databases
    d. Other, please specify
6. Is there any cross-check of data with other databases?
7. If yes, what is the common key?
8. Are there explicit rules and regulations as to how government agencies can link their databases? Yes/no
9. Is there an explicit list of institutions that are allowed to access the ID database? Yes/no
10. Is there a standard format for MOUs between the ID issuing agency and other government agencies? Yes/no

D.3 Ubiquity/Portability

11. Is the ID system valid/recognized in the whole country?
12. Is it recognized in neighboring countries?
13. How many social protection programs are using this ID?
14. Is this ID used commonly for any of the following purposes?
    a. Opening a bank account
    b. Obtaining credit or loans
    c. Reporting to the tax authority
    d. Obtaining marriage certificate
    e. Obtaining private health insurance
    f. Enrolling in social insurance programs
    g. Qualifying for cash transfers, food, or other safety net programs
    h. Getting a cell phone account
    i. Obtaining a passport
    j. Getting a driver's license
    k. Voting
    l. Registering a vehicle
    m. Purchasing property
    n. Other, specify

Criterion E: Governance and Respect of Rights and Dignity

E.1 Governance Framework

1. Is there a clear partition of the roles and responsibilities for implementation and oversight of the identification system?
2. What is the name of the agency that is responsible for issuing this ID?
3. Is this an independent agency (i.e.., not part of another agency or ministry)?
4. If no, to what ministry or other government entity does it report?
5. Is this agency involved in the civil registration?
6. Do this agency manage different ID systems?
7. Is there a national commission of any other body that is looking at identification and/or databases on individuals?

8. If yes, how can this body intervene?
9. Is there a mechanism to ensure the participation of social partners?
10. Is there a mechanism to ensure the participation of representatives of vulnerable groups of the population?

E.2 Institutional Capacity

11. What is the annual budget of the agency in charge of issuing the ID?
12. Where does this budget come from (general revenue, donor funded, etc.)?
13. What is the cost of issuing one ID?
14. What is the estimated annual budget directly related to issuing IDs?
15. How many branch offices does the agency have?
16. How many employees/staff?
17. How many employees/staff are directly involved in issuing IDs?
18. Is there an operations manual that documents the ID issuance process?
19. How many employees/staff are dedicated to the maintenance of the database?
20. Are database maintenance and operations documented in a manual?
21. How are the capacities of the staff developed?
22. Are the required IT infrastructures in place?

E.3 Respect for Rights and Dignity

23. Is there legislation on privacy or protection of personal data that delimits the access and use of data? Are there explicit rules and/or regulations on the possible use of information stored in the ID database? Are there penalties for violations? Yes/no
24. Is there an explicit list of institutions that are allowed to access the ID database?
25. Is there a standard format for MOUs between the ID issuing agency and other government agencies? Yes/no
26. Has a privacy impact assessment ever been conducted? Yes/no
27. Is public reporting of exceptional cases of accessing data (e.g., based on national security threats) required? Yes/no
28. Is there a supervisory body within government responsible for monitoring compliance with privacy and data protection rules that apply to this ID database?

29. Is the process for grievance redress for individuals who claim their privacy was violated clear? Yes/no
30. Is the information that must be provided for obtaining this ID the minimum required for its purposes? Yes/no
31. How are data encrypted (when at rest/when in motion)?
32. Is all access to computers and data systems within the ID environment assigned and tracked?
33. Are security systems and processes regularly tested?
34. What other measures are taken to ensure networks, systems, and applications are secure?
35. Which of the following procedures or policies are in place?
    a. Information security and management policy
    b. Information security organization structure policy
    c. Risk assessment policy and procedures
    d. Asset classification policy and procedure
    e. Asset classification and control standard
    f. Information labeling and handling procedure
    g. Acceptable use guideline
    h. Procedure for control of documents and records
    i. Human resources security policy and procedure
    j. Physical and environmental security policy and procedure
    k. Change management policy and procedure
    l. Third-party management policy and procedure
    m. Antivirus and malicious software policy and procedure
    n. Backup and restore policy and procedure
    o. Network security policy and procedure (including Internet, intranet, mobile computing, teleworking, firewall security)
    p. Media-handling policy and procedure
    q. Monitoring policy and procedure
    r. Access control policy and procedure (including password security)
    s. Network access control policy and procedure
    t. Systems development maintenance policy and procedure
    u. Incident management policy and procedure
    v. Business continuity management policy and procedure
    w. Cryptographic procedure document
    x. Minimum baseline security standards

ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

OVERVIEW OF FINDINGS

DELIVERY

The assessment criteria elaborated above should then be applied to the key areas. The assessment results should be captured in an overview table (overview of findings that captures key strengths and weaknesses in the performance of the identification system. The table below provides guidance on how to use the criteria and assess the performance from weaker to stronger.

Illustration of ID and CR System Assessment Results

	Latent	Emerging	Moderate	Advanced
Accessibility • Coverage • Inclusiveness • Appropriateness – Cost of access and other barriers to access – Enrollment approach active or passive	Minority of the eligible population has an ID that can be used by the program Some vulnerable groups are de facto excluded from the ID system Acquiring the ID is costly in relative terms and administratively cumbersome (passive enrollment approach)	Most of the eligible population has an ID that can be used by the program Acquiring the ID is a burden for some groups of the population (e.g., the poor) Barriers to access are known (passive enrollment approach) and a strategy is defined	Almost all eligible people have the required ID Process of obtaining the ID involves low costs Concrete actions are taken to ensure access to the ID for vulnerable groups (active enrollment)	All eligible people have or can easily obtain the form of ID required for the program (including the poor, noncitizens, indigenous groups, etc.) A process is defined for the timely inclusion of newborns in the system The cost of obtaining the ID is low, and there are no other barriers to obtain the ID
Robustness • Uniqueness/accuracy • Security • Effective and reliable authentication procedures	Duplicates and other errors in the database are a major concern, as there is no process for deduplication and data cleaning Very low rates of birth and death registration/ civil registry very unreliable IDs are easily falsified Very weak institutional capacity to ensure database security Authentication process very unreliable/ dysfunctional	Some quality control and database maintenance but mostly paper-based recordkeeping Civil registry is functional, but low rates of birth and death registration and significant delays in registration Security measures are rather weak, and IDs can be falsified Authentication process unreliable	Data quality and deduplication protocols are in place and the database is reasonably accurate The majority of births and deaths is registered, and the civil registry works well with minimal delays Database security measures are in place, and IDs are rarely falsified Basic authentication processes	Electronic records facilitate quality control and deduplication; errors are minimal All births and deaths are registered in a fully functional civil registry that works with minimal delays Strong database security controls Very difficult to produce fraudulent IDs Good authentication standards applied

	Latent	Emerging	Moderate	Advanced
Costs of the ID system • Information technology • Maintenance • Ease of operation; administrator training	High cost Cost are disproportional compared to the benefits provided			Low cost ID costs are reasonable compared to the benefits provided
Interoperability and portability • Interoperability • Portability	There is no standardized data format and little or no database linkages across programs; high dependence on local knowledge (e.g., community) and references for verifying identity The ID can be used only for one purpose and is tied to one locale	Some data are standardized, and a few major programs aim to make their databases compatible or use a common ID platform; difficult to track one individual across different programs There is a process to access benefits across the country, but it requires complicated administrative procedures and takes time	Most data are standardized, and some SP programs use a common ID Most program management information systems can be linked Accessing benefits at different points across the country requires paper work but is possible	To the extent that this is desired, interoperability across programs is fully functional, or SP programs use a common ID at the national level

	Latent	Emerging	Moderate	Advanced
Governance and Respect of Rights and Dignity. • Governance framework • Institutional capacity • Respect for rights and dignity – Data protection – Effective and accessible redress mechanisms in case of abuse, lack of due diligence, or wrongdoing	Roles and responsibilities for ID are not clearly assigned, and the ID process is not well implemented Infrastructure and the number and skills of staff are entirely insufficient Ad hoc or nonexistent mechanisms for privacy and data access No redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing	Roles and responsibilities are assigned to certain institutions, but they do not perform their functions as foreseen Infrastructure and the number and skills of staff allow ID processes to be carried out only partially Minimal protocols in place for personal data protection and privacy Redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing, but are not effective and accessible	The institutional and administrative framework clearly assigns roles and responsibilities, but there are complaints regarding delays and irregularities in implementation Infrastructure and the number and skills of staff are sufficient to carry out most of the ID process Most internationally accepted personal data protection standards and protocols are followed Mostly effective and accessible redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing	An effective institutional and administrative framework clearly assigns and enforces roles and responsibilities Infrastructure and number and skills of staff are sufficient to adequately carry out all ID processes Full compliance with internationally accepted personal data protection guidelines Fully effective and accessible redress mechanisms in place in case of abuse, lack of due diligence, or wrongdoing

ISPA
INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

IDENTIFICATION SYSTEMS
FOR SOCIAL PROTECTION

COUNTRY REPORT OUTLINE

DELIVERY

The primary output of the assessment will be a country report. This report should be about 35 pages long and should generally adhere to the following outline.

Preface

- Description of the motivation for the assessment and the program(s) to be assessed
- Assessment team and dates of the assessment

1. Background

- Summary of the rationale for carrying out the assessment.
- Brief reference to the ID system(s) to be evaluated and description of key features
- Description of key sources of information and data used for the assessment

2. Country context

- Snapshot of institutional arrangements, legal framework, and main SP and ID system actors
- Snapshot of SP in the last 10 years
- Snapshot of the ID systems in the last 10 years
- Snapshot of the human development and poverty profile of the country
- Key indicators relevant for ID, including income level, demographic structure, urban/rural split, literacy rates, etc.
- Citations and cross-references to the country's major SP and labor programs and their coverage (table 1)
- Tabular presentation of key indicators (listed below) of the ID ecosystem; if ID systems from different programs are included in the assessment, repeat the table for each system
    - Estimated coverage of foundational ID(s) where relevant

Table 1 Country SP Programs at a Glance

(Provide information for the most relevant SP programs operating in the country.)

Item	Program A	Program B	Program C	....
Program/benefit category				
Risk covered/function				
Targeted population group				
Objective				
Qualifying conditions				
Benefit level/beneficiary				
Responsible implementing agency				
Geographical areas covered				
Payment mechanism (if cash or near cash)				
Number of beneficiaries (value/latest year)				
Total expenditure (local currency unit) (value/latest year)				

- Estimated coverage of program ID
- Type of ID and functional use
- Estimated costs of the current ID system
- Biometrics captured (none; fingerprints and if so, how many; iris; other)
- Medium for and centralization of ID database (paper/electronic; decentralized/centralized)
- Whether the ID is unique to an individual
- Form of verification of ID by program at point of transaction

3. **Assessment**

- Detailed narrative based on responses to the questionnaire and interviews with the relevant agencies covering system performance strengths and weaknesses in accordance with the assessment criteria across the five key areas

- Summary of assessment captured in Overview of Findings

4. **Policy Options**

- Description of the most cost-effective options available to the country for improving the ID system(s), taking into account its starting point and initial conditions
- References to relevant international experience and technical annexes as appropriate

5. **Conclusions**

- Summary of key performance strengths and weaknesses and costs of the ID system(s)
- Discussion of areas for future research and/or attention
- Caveats regarding information quality and availability

INTER AGENCY
SOCIAL PROTECTION ASSESSMENTS

ISPATools.org