



VERSION 1.0

PRACTITIONER'S GUIDE

October 2019



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

Some Rights Reserved

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

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

Rights and Permission



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

Attribution—Please cite the work as follows: World Bank. 2019. ID4D Practitioner’ Guide: Version 1.0 (October 2019). Washington, DC: World Bank. License: Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

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

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

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

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

Disclaimer

This ***Practitioner's Guide*** is a reference document to be consulted by governments, development partners, academics and others when considering, designing, implementing, or managing a foundational digital identification (ID) system. It is *not* intended to be a Guide for planning World Bank operations.

This Guide is based on evolving international good practice, as understood by the World Bank's Identification for Development (ID4D) initiative. It reflects experiences in a range of countries from different regions, with different legal systems, and at different stages of economic development. It also takes into account existing literature, international conventions, and norms and principles (including the *Principles on Identification*, available at: <http://id4d.worldbank.org/principles>).

There is no guarantee that addressing all the issues raised in this Guide will result in successful ID system in a country—that will depend on many factors that must be considered, and which may be different from country to country. While every attempt has been made to be complete, there may be issues affecting the design, establishment of operation of an ID system that are not addressed in this Guide, or that are addressed in the context of certain assumptions, facts and circumstances that do not apply equally to every situation. This Guide is a reference tool only.

Version History

Release	Format	Date	Details
Draft for consultation	PDF	June 2019	Beta release of the Guide for initial public consultation and feedback.
Version 1.0	PDF, web, print	October 2019	Incorporated feedback from consultation draft.

Contents

Disclaimer	iii
Version History	iv
Contents.....	v
Tables.....	vii
Figures	viii
Boxes.....	ix
About ID4D.....	x
Abbreviations	xi
Acknowledgements	xiii
About this Guide.....	xiv
Scope	xiv
Organization	xv
References	xvi
SECTION I. Introduction	0
Why ID matters for development.....	1
Good ID supports multiple development goals.....	2
Creating a good ID system presents risks and challenges, but there are common success factors	5
ID 101: Basic concepts.....	11
Types of ID systems	12
Identity lifecycle.....	17
Stakeholders and roles	21
SECTION II. Designing an ID System.....	24
1. Principles.....	26
Pillar 1: Inclusion.....	26
Pillar 2: Design	27
Pillar 3: Governance.....	29
2. Planning Roadmap.....	31
Understand the Status Quo	32
Define Vision	38
Identify Constraints	41
Evaluate Costs and Benefits.....	47
Assess Risks	52
3. Key Decisions	61
4. Procurement.....	62
SECTION III. Topics.....	65
Legal Framework.....	66
Enablers	66
Safeguards.....	67
Public Engagement	81
Public consultation	81

Communications	83
Grievance redress	85
Privacy & Security	87
Encryption	90
Digital certificates and PKI	92
Tokenization	94
Platforms for personal oversight	97
Tamper-proof logs	98
Operational security controls	100
Implementing a cybersecurity program	102
Administration	104
ID authority and governance structure	105
Roles and responsibilities	109
Business models	111
Data	118
Biographic data	119
Biometric data	122
IT Systems	129
Hosting options	129
Registration & Coverage	135
Eligibility	136
Registration strategy	139
Registration operations	146
Proofing identity claims	150
Credentials & Authentication	156
Types of credentials and authenticators	157
Credential Issuing	168
Authentication mechanisms	170
Levels of assurance (LOAs)	176
Interoperability	179
Interoperability frameworks	183
Linking ID and civil registration	184
Mutual recognition of IDs across borders	187
Standards	193
Technology standards	195
Data standards	198
SECTION IV. Resources	200
ID4D Tools and Research by Topic	201
Other References and Resources	208
Glossary	214

Tables

Table 1. ID Stakeholders, roles, and objectives	22
Table 2. Principles on Identification for Sustainable Development	26
Table 3. Identity ecosystem stock-taking	32
Table 4. Design implications of existing ID ecosystem and stakeholders	33
Table 5. Design implications of status quo ID coverage	35
Table 6. Design implications of the robustness of existing ID systems	36
Table 7. Design implications of existing legal framework	38
Table 8. Design implications of potential cross-cutting goals for ID system	38
Table 9. Design implications of specific use cases	40
Table 10. Design implications of digital infrastructure	42
Table 11. Design implications of geography	44
Table 12. Design implications of socioeconomic development	45
Table 13. Design implications of cultural and historic factors	46
Table 14. Design implications of timeline constraints	47
Table 15. ID system features that generate savings in the public sector	51
Table 16. Threats to privacy and data protection throughout the identity lifecycle	53
Table 17. Common vulnerable groups and barriers to registration and use of ID	58
Table 18. Examples of Key Decisions for ID systems	61
Table 19. Potential methods of public consultation	82
Table 20. Communication format and channels	83
Table 21. Examples of privacy and data protection enhancing technologies and operational controls	89
Table 22. Example requirements for data encryption in an identity system	92
Table 23. High-level checklist for the physical security of ID systems	101
Table 24. Institutional arrangements for ID authority	106
Table 25. Governance models for ID providers	107
Table 26. Example of fees for verification and authentication services	112
Table 27. Types of data and evidence often collected by an ID system	118
Table 28. Comparison of biometric technologies commonly used in ID systems	123
Table 29. Comparison of data storage options	131
Table 30. Insourcing and Outsourcing Registration	144
Table 31. Example measures and technologies used in identity validation	151
Table 32. Comparison of common card types	162
Table 33. Offline authentication mechanisms for in-person transactions	173
Table 34. Examples of online authentication mechanisms for in-person and/or remote transactions	174
Table 35. Example levels of assurance	178
Table 36. Requirements for building interoperability frameworks	183
Table 37. Comparative data standards for India, EU and ICAO	198

Figures

Figure 1. Unregistered population by region	1
Figure 2. Building blocks of digital ID systems	5
Figure 3. The basic roles of ID systems	11
Figure 4. Classification of government ID systems	13
Figure 5. Potential role of a foundational ID system	15
Figure 6. Identity lifecycle	18
Figure 7. Common authentication factors	20
Figure 8. Major cost categories for ID systems	48
Figure 9. Cost categories and drivers for ID systems	49
Figure 10. Savings and revenue-generation mechanisms	51
Figure 11. Key considerations for public engagement.....	81
Figure 12. Privacy frameworks for personal data.....	88
Figure 13. Digital certificates	93
Figure 14. Tokenization vs. encryption.....	96
Figure 15. Key considerations for the institutional home and governance of the ID authority.....	109
Figure 16. Example institutional roles within an ID system.....	110
Figure 17. Key considerations for roles and responsibilities.....	111
Figure 18. Key considerations for charging fees for ID services	114
Figure 19. Key considerations for private-sector partnerships in ID systems.....	117
Figure 20. Key considerations for the types of data collected	119
Figure 21. Key considerations for using biometrics.....	125
Figure 22. Key considerations for data storage.....	134
Figure 23. Registration strategies for different stages of the lifecycle.....	140
Figure 24. Key considerations for identity proofing.....	151
Figure 25. Example deduplication process using biometrics.....	155
Figure 26. Key considerations for credentials and authentication.....	156
Figure 27. Examples of credentials and authenticators commonly issued by foundational ID systems	157
Figure 28. ID number structure	160
Figure 29. Digital authentication modes.....	171
Figure 30. Types of interoperability in an ID system.....	180
Figure 31. Interoperability between CR and ID for death notifications.....	186
Figure 32. Linking ID creation to birth registration	186
Figure 33. Web-based mutual recognition—example architecture and workflows.....	189
Figure 34. API-based mutual recognition—example architecture and workflows.....	190
Figure 35. Offline mutual recognition—example architecture and workflows.....	191
Figure 36. Technical standards decision tree	197

Boxes

Box 1. Identity is instrumental for multiple SDGs	2
Box 2. Spotlight on identification in social protection	4
Box 3. Additional ID4D publications.....	10
Box 4. Defining “proof of legal identity”	13
Box 5. Defining privacy and data protection in the ID system context.....	52
Box 6. RFP Checklist.....	64
Box 7. Planning Tools.....	64
Box 8. EU General Data Protection Regulation (GPDR)	69
Box 9. Examples of data privacy and protection oversight agencies.....	71
Box 10. Examples of security breach notification laws.....	73
Box 11. Examples of data sharing arrangements.....	74
Box 12. GPDR limits on data transfers	75
Box 13. Examples of user consent laws.....	76
Box 14. Examples of legal measures for inclusion.....	79
Box 15. Additional resources on legal frameworks.....	80
Box 16. Examples of Information and education campaigns	84
Box 17. Examples of grievance redress mechanisms.....	85
Box 18. Foundational Principles of Privacy by Design (PbD).....	87
Box 19. Understanding public-key encryption and digital signatures.....	90
Box 20. Austria’s sector-specific identifiers	95
Box 21. India’s Virtual ID and tokenization systems.....	96
Box 22. Estonia’s citizen portal.....	98
Box 23. Tamper-proof logs in Estonia	99
Box 24. Temporary institutional arrangements for the startup phase of an ID system	108
Box 25. PPP example in Moldova	116
Box 26. Additional resources on ID system administration	117
Box 27. Examples of minimum sets of personal data.....	120
Box 28. Examples of policies regarding sensitive data	121
Box 29. Examples of incorporating children into an ID system with biometrics or alternative methods of establishing uniqueness	127
Box 30. Country Experiences with ID and Nationality	137
Box 31. Examples of the inclusion of children in ID systems.....	138
Box 32. The relationship between mass registration and population (statistical) censuses.....	142
Box 33. Examples of inclusive identity proofing processes	153
Box 34. Examples of multiple types of credentials in one country	158
Box 35. Selective attribute disclosure in the German eID system	165
Box 36. Moldova’s Mobile eID	166
Box 37. The Austrian virtual Citizen Card.....	168
Box 38. GOV.UK Verify.....	176
Box 39. NIST levels of assurance for digital ID	177
Box 40. Estonian X-Road Model.....	181
Box 41. Understanding CR and ID	185
Box 42. The European Union electronic Identification, Authentication and trust Services (eIDAS) regulation ..	188
Box 43. Proposal for mutual recognition of national IDs in the East African Community (EAC)	192
Box 44. Vendor and technology neutrality.....	194
Box 45. Examples of standards use.....	195

About ID4D

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

The mission of ID4D is to enable all people to access services and exercise their rights, by increasing the number of people who have trusted proof of legal identity. ID4D makes this happen through its three pillars of work:

- Thought leadership and analytics to generate evidence and fill knowledge gaps;
- Global platforms and convening to amplify good practices, collaborate, and raise awareness; and
- Country and regional engagement to provide financial and technical assistance for the implementation of inclusive and trusted digital identification systems that are linked with civil registration.

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

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

Abbreviations

AAL	authenticator assurance level
ABIS	automated biometric identification system
AFIS	automated fingerprint identification system
API	application program interface
BOT	build-own-transfer
CA	certificate authority
CBA	cost-benefit analysis
CDD	customer due diligence
CERT	computer emergency response team
CR	civil registration
CRVS	civil registration and vital statistics
DPIA	data protection impact assessment
FAL	federation assurance level
FIP	Fair Information Practice
FNM	false non-match
FNMR	false non-match rate
FTC	fail to capture
FTE	failure to enroll
G2P	government to person
GDPR	General Data Protection Regulation
IAL	Identity assurance level
ICT	information and communications technology
ID	identification, identity document
IDEEA	ID Enabling Environment Assessment
IEC	Information and education campaign

(e)KYC	(electronic) know-your-customer
LOA	level of assurance
MFA	multi-factor authentication
MNO	mobile network operator
NFC	near field communication
NGO	non-governmental organization
PbD	Privacy by Design
PETs	privacy-enhancing technologies
PII	personally identifiable information
PIN	personal identification number
PKI	public key infrastructure
PPP	public-private partnership
OTP	one-time password
RENIEC	<i>Registro Nacional de Identificación y Estado Civil (Peru)</i>
RFID	radio frequency identification
RFP	request for proposals
SAML	Security Assertion Markup Language
SDG	Sustainable Development Goal
SIM	subscriber identification module
SLA	service-level agreement
SSN	social security number
TLS	Transport Layer Security
UIDAI	Unique Identification Authority of India
UIN	unique ID/identity number
USSD	unstructured supplementary service data
VPN	virtual private network

Acknowledgements

This Guide was drafted by Julia Clark for the World Bank’s Identification for Development (ID4D) Initiative under the leadership of Vyjayanti Desai and with significant contributions from World Bank staff and expert consultants, including Adam Cooper, Jonathan Marskell, Anita Mittal, James Neumann, David Satola, and Michiel van der Veen. Many others—including Jerome Buchler, Luda Bujoreanu, Nils Junge, Victoria Esquivel Korsiak, Knut J. Leipold, Anat Lewin, Vlad Manoil, Samia Melham, Anna Metz, Julian Najles, Robert Palacios, and Emmanuel Vassor—also provided important inputs and reviews.

This Guide draws extensively on existing ID4D publications—available at id4d.worldbank.org and detailed in Section IV of the Guide—and would not have been possible without the work of these previous authors. In particular, it builds upon the 2014 Digital ID Toolkit for Africa, which was prepared by Joseph J. Atick (ID4Africa) and Zaid Safdar (World Bank).

Finally, this Guide has benefited from reviews, feedback, and inputs from Alan Gelb (Center for Global Development), Thampy Koshy and his team (Ernst & Young), representatives of the Secure Identity Alliance (SIA), Sanjay Dharwadker (WCC), Tom Flemming (EBRD), Jeremy Grant (FIDO Alliance), Yesha Tshering Paul, Prakriti Singh and Amber Sinha (CIS, India), and Edgar Whitley (LSE).

This work is a product of the staff of the World Bank with external contributions. The findings, interpretations, and conclusions expressed do not necessarily reflect the views of the World Bank, its Board of Executive Directors, or the governments they represent. The World Bank does not guarantee the accuracy of the data included in this work.

About this Guide

This Guide was created by the World Bank Group's [Identification for Development \(ID4D\) Initiative](#) to help practitioners design and implement identification (ID) systems that are inclusive and trusted—in accordance with the ten [Principles on Identification for Sustainable Development](#) and other international standards and good practices. It is intended to serve as a central resource for country counterparts, World Bank Group staff, and other actors involved in planning, managing, and financing ID systems. The Guide builds on existing resources and publications from ID4D and other organizations and is intended to help readers navigate this disparate material in a user-friendly way.

Rather than advocating for any specific model of identity provision, this Guide presents key decisions and good practice technical options relevant for designing an entirely new ID system or improving an old one. It then offers analysis and links to more in-depth tools to assess the fitness of different design choices for different contexts and goals.

To access the web version of this Guide or to download the most recent PDF, visit id4d.worldbank.org/guide

This Guide is meant to be a living document that will be updated periodically to reflect new lessons, standards, and resources. It is available in a PDF version (which you are reading now) and a web-version for improved accessibility and readability. The most recent web and PDF versions of the Guide can be found at <http://id4d.worldbank.org/guide>. Feedback to help us improve the content is always welcome and can be submitted to id4d@worldbank.org.

SCOPE

The focus of this Guide is on the design and implementation of ID systems that provide people with proof of their legal identity, which is commonly needed to access basic services, rights, and protections. Therefore, the Guide applies primarily to foundational ID systems—such as civil registries, national IDs, population registers, etc.—created to serve as authoritative sources of legal identity information for the general population and to provide proof of identity for a variety of public and private sector use cases. However, much of the material provided in this Guide will also apply to the design and implementation of functional ID systems that are created to manage identities for specific sectors or uses, such as taxation, voter registration, social benefits, refugee status determination, and more.

To avoid duplicating the considerable work published by the United Nations and other actors as part of global and regional initiatives on civil registration and vital statistics (CRVS), **this Guide does not cover the development of civil registration (CR) systems on their own.** However, given that building a strong CR is critical to providing proof of legal identity from birth and for ensuring the accuracy, sustainability, and efficiency of other ID systems, the Guide includes topics on the linkages between CR and other foundational ID systems.

As the world becomes increasingly digital, so have foundational ID systems—the Guide reflects this trend by **focusing on digital (or “digitalized”) foundational ID systems**. In addition to those provided directly by the government, this includes forms of digital ID that are provided in partnership with or outsourced to the private sector but which are linked to a person’s “official” or “legal” identity and recognized by the government for use in official purposes (e.g., for online government services). However, **it does not discuss many other types of digital ID systems, such as those provided by the private sector for customer authentication (e.g., log-ins for email accounts or social media), or refer to the broader notion of “who you are on the internet.”** Throughout this Guide, the term “digital ID” is used synonymously with “digital/digitalized foundational ID systems” unless otherwise noted.

ORGANIZATION



The Guide is organized into four parts:

- **SECTION I: Introduction.** The Guide begins with a discussion of **why identification matters for development**, as well as key benefits, risks, and success factors. It also includes a primer on **common identity-related terms and processes**.
- **SECTION II: Designing an ID System.** The second section of the Guide walks through important stages of planning an ID project. It begins with an overview of the ten **Principles on Identification** that provide high-level design guidance, and then presents a **planning roadmap** for assessing the country- and context-specific factors that should shape system design. Next, it summarizes the **key decisions** that practitioners need to make to define the scope and functional architecture of their ID project. Finally—once key decisions have been made through the planning process—the section concludes with guidance on **procurement**.
- **SECTION III: Topics.** This section provides overviews of important ID-related technologies, processes, institutions, and other topics throughout the identity lifecycle. This includes a more **detailed explanation of the options discussed under Section II. Key Decisions**, as well as other subjects crucial to planning and operating an ID system: (1) legal and regulatory framework, (2) public engagement, (3) privacy and security, (4) administration, (5) data, (6) IT systems, (7) registration & coverage, (8) credentials & authentication, (9) interoperability, and (10) standards.
- **SECTION IV: Resources.** The final section of the Guide provides **additional resources**, including an annotated list of the ID4D materials that provide a deeper dive into particular topics, resources from other organizations and a glossary of identity-related terms used throughout the Guide.

Completing each step in **Section II. Planning Roadmap** will help ensure that an ID system is aligned with the country's goals, priorities, and capacities, and help mitigate key risks.

REFERENCES

For ease of navigation, the following notation is used throughout the text of the Guide:

- **References to other sections of this Guide** are highlighted in blue (e.g., see **Section III. Data > Biographic data**).
- **References to publications and resources** are highlighted in orange (e.g., see **ID4D Global Dataset**). Note that ID4D materials—cited frequently throughout the text—are referred to by their name for ease of reference, while external publications and resources are cited using the author-date format.

Descriptions of ID4D materials and a full list of external references are provided in **Section IV. ID4D Tools and Research**.

SECTION I. Introduction

 INTRODUCTION	 Motivation Why identification matters for development and challenges to creating “good” ID systems	 ID 101 Basic terminology on ID, the identity lifecycle, types of ID systems, and stakeholders and roles
--	---	--

This section provides a primer on identification for development that we hope is useful for development practitioners and others who are new to thinking about identification, and for identity experts who are new to thinking about development.

It begins with an overview of **why identification matters** for development, including the global identification gap, the role of ID in supporting multiple development goals, and the particular risks, challenges, and success factors in building an inclusive and trusted ID system.

It then **introduces core identity-related concepts and terms** referenced throughout the Guide, including different types of ID systems, the lifecycle of creating and managing identities. and the main stakeholders and roles involved in providing, using, and overseeing ID systems.

Contents:

- [Why identification matters for development](#)
- [ID 101: Basic concepts](#)

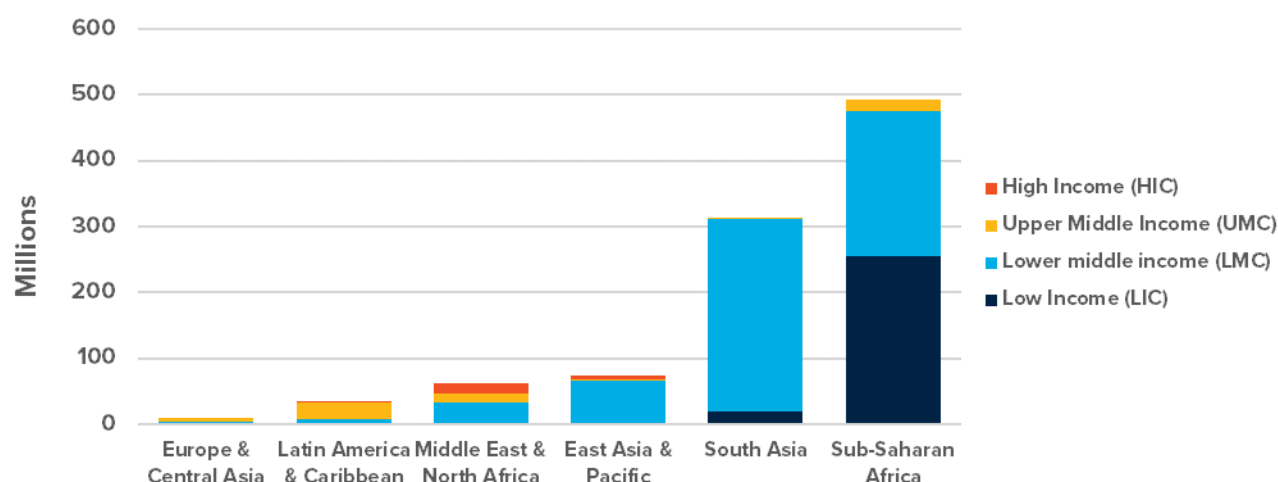
WHY ID MATTERS FOR DEVELOPMENT

As of 2018, the ID4D Global Dataset estimates that there are 1 billion people worldwide who do not have basic identity documents. These people are overwhelmingly in Sub-Saharan Africa and South Asia and are typically members of the poorest and most vulnerable groups, including marginalized women and girls, less-educated people, migrants, refugees, asylum seekers, stateless persons, people with disabilities, and people living in rural and remote areas (*ID4D-Findex*).

Nearly one-in-two women in low income countries do not have their country's national ID or similar foundational document, limiting their access to critical services and participation in formal political and economic life (*ID4D-Findex*). Half—nearly 500 million—of those without basic proof of legal identity live in Sub-Saharan Africa, and 47 percent are children who were not registered at birth (*ID4D Global Dataset*).

For more data on the global identification gap, visit id4d.worldbank.org/global-dataset

Figure 1. Unregistered population by region



Source: *ID4D Global Dataset (2018)*

This global identification gap is partly a result of the fact that many low- and middle-income countries lack well-functioning civil registration (CR) systems to record births, deaths, marriages, and other vital events, which are essential for providing legal identity from birth. Even where civil registers and ID systems do exist, they are often paper-based, subject to data errors and fraud, built for narrow purposes that do not suit more general uses (e.g., voter ID cards or social benefit numbers), fragmented across several government agencies, and/or exclusionary of specific groups or populations. Furthermore, many countries lack strong legal and regulatory frameworks to support trusted and inclusive ID systems that adequately ensure privacy and data protection. **Thus, in addition to the 1 billion people who do not have basic proof of identity, many more lack ID that is useful and trusted. Without trust and convenience for people and other users, these ID systems have diminished value.**

Good ID supports multiple development goals

Why does the identity gap ID matter? Inclusive and trusted—i.e., “good”—ID systems are crucial tools for achieving sustainable development, including the World Bank Group’s twin goals of ending extreme poverty and boosting shared prosperity. For this reason, **ensuring that everyone has access to identification is the explicit objective of [Sustainable Development Goal \(SDG\) Target 16.9](#)**—to “provide legal identity for all, including birth registration” by 2030.

Furthermore, identification is also a key enabler or contributor to many other SDG targets, such as financial and economic inclusion, social protection, healthcare and education for all, gender equality, child protection, agriculture, good governance, and safe and orderly migration (see Box 1). For these reasons, identification is widely-recognized as being instrumental to realizing the SDG promise to “leave no one behind.”

Box 1. Identity is instrumental for multiple SDGs

In addition to **SDG Target 16.9**, the ability of individuals to prove their identity—and the ability of service providers to identify beneficiaries and customers—is either **a direct or indirect enabler of many other SDGs**. For example, ID is either essential or helpful for achieving many of the goals and targets related to:

Access to finance

- Satisfy know-your-customer (KYC) requirements for banking — Goal 1 and Target 1.4
- Provide a unique ID for credit registries — Targets 1.4 and 8.3
- Improve integrity and reduce the costs of remittance transfers — Target 10c
- Prove ownership over property — Goal 1 and Target 1.4
- Improve land access and targeted services for small-holder farmers — Target 2.3

Gender equality and empowerment

- Full participation in economic and social life — Goal 5
- Equal access to economic and financial resources — Target 5a
- Enhancing the use of technology for empowerment — Target 5b
- Eliminating trafficking of women and girls — Target 5.2

Access to basic health and education services

- Unique ID for health insurance — Target 3.8
- Tracking of TB and HIV/AIDs treatment — Target 3.3
- End preventable deaths of newborns via CR health data — Target 3.2
- Higher childhood vaccination rates — Goal 3 and Target 3.3
- Registration and school exams — Goal 4

Child protection

- Help eliminate child labor through proof of age — Target 8.7
- Help end child marriage through proof of age — Target 5.3

Migration and labor market opportunities

- Reduce transaction costs in hiring — Goal 8 and Target 8.5
- Facilitate safe and responsible migration and mobility — Goal 10 and Target 10.7

Improved access and quality of social protection

- Improve targeting, timeliness, cost-effectiveness of payments — Goal 1 and Target 1.3

- Improve transparency and reduce leakage — Target 1.3
- Facilitate fast and efficient delivery of emergency aid — Target 1.5
- Phase out harmful fuel subsidies by moving to direct cash payments — Target 12c

Governance

- Remove ghost workers and generate public savings — Goal 16 and Target 16.5
- Widen tax base and reduce tax fraud — Target 17.1
- Clean voter registry and reduce voter impersonation—Target 16.7

Source: Adapted from *Gelb and Diofasi (2018)*, Chapter 3, and *The Role of Identification in the Post-2015 Development Agenda Digital Identity*

Inclusive and trusted ID systems can help achieve these goals by:

- **Empowering individuals and enhancing their access to rights, services, and the formal economy.** With proof of identity, individuals are empowered to access basic [financial](#), [health](#), and social services for which identification is often a prerequisite (see Box 1). The ability to prove your identity or particular attributes (e.g., age) is also essential to accessing key rights, such as voting and the [prevention of child marriage](#), as well as economic opportunities such as labor mobility, formal employment, and property rights. These opportunities and protections are particularly necessary for vulnerable populations who are also least likely to have proof of identity, including those living in poverty, [marginalized women and girls](#), inhabitants of rural and remote areas, [refugees, stateless populations, and migrants](#).
- **Strengthening the transparency, efficiency, and effectiveness of governance and service delivery.** Central to a government's ability to deliver services to its people—including education, healthcare, safety nets, pension payments, land registration, agricultural extension, and more—is knowledge of who those people are and relevant attributes (see Box 2). For governments, ID systems therefore play an important role in enhancing the capacity to ensure that government to person (G2P) transfers, such as [cash transfers, wages, and subsidies](#), reach their intended beneficiaries, and are not subject to leakage or fraud. Digital ID systems can also improve services by creating a foundation on which to build new modes of delivery, including e-government and direct benefits transfers and increasing the overall efficiency of administration.
- **Supporting private sector development and service delivery.** As in the public sector, private enterprises also have identification and authentication needs for their clients. For example, a bank's ability to offer services—such as [opening a bank account](#) or securing a loan—requires a certain knowledge about a prospective client's identity and the ability to ensure that they are interacting with the same person (and not an identity thief) over time. Trustworthy ID credentials can thus [reduce operating costs for private firms](#) associated with identity verification for regulatory compliance (e.g., know-your-customer or customer due diligence requirements), widen customer bases, generate new markets, and support a business-friendly environment more broadly.
- **Growing the digital economy.** Given the fundamental need for secure and accurate online identification and authentication, digital ID and other trust services—such as e-signatures—form part of the core foundation or a “stack” needed for successful digital economies. When enabled by digital infrastructure that brings people and organizations online, digital ID and

trust services can be leveraged by government and commercial platforms to facilitate a variety of digital transactions, including digital payments. Together, digital ID and payments platforms provide the means to move towards a cashless society, creating productivity gains, reducing corruption and fraud, and further improving user convenience.

- **Regional and global integration.** With economies and societies becoming more integrated across the world, identification can accelerate these physical and digital connections. Physical or digital foundational IDs can be recognized as a travel document in lieu of a passport, which can streamline travel and make migration more accessible. Similarly, digital IDs issued by one country can be recognized by other countries, enabling trusted transactions to take place across borders (e.g. entering contracts or registering businesses), thereby boosting the economic and social inclusion of migrants and facilitating trade.
- **Generating reliable and continuous statistics to measure progress and inform policy.** Civil and population registers are a critical administrative sources of demographics and vital statistics, which in turn provide essential evidence to support the ability of governments and the private sector to engage in long-term planning and policy making in areas such as [public health](#) and infrastructure. For example, civil registration—with inputs from the health sector—enables policymakers to monitor cause of death and maternal and infant mortality rates and to rapidly respond to epidemics (e.g., HIV/AIDS and non-communicable diseases).

Box 2. Spotlight on identification in social protection

When ID systems are weak, people may have difficulty proving who they are and/or their eligibility for social protection programs such as cash transfers, pensions, ration cards, social insurance, and other benefits. This problem is compounded by the fact that those most in need of this assistance are also those least likely to have an ID, including poor, rural, and marginalized people. Furthermore, if their ID is linked to a financial address to receive payments on any channel (e.g. bank accounts or mobile money), this facilitates interoperability, gives choice, and enhances convenience to beneficiaries in cases when they change their account or preferred payment mechanism.

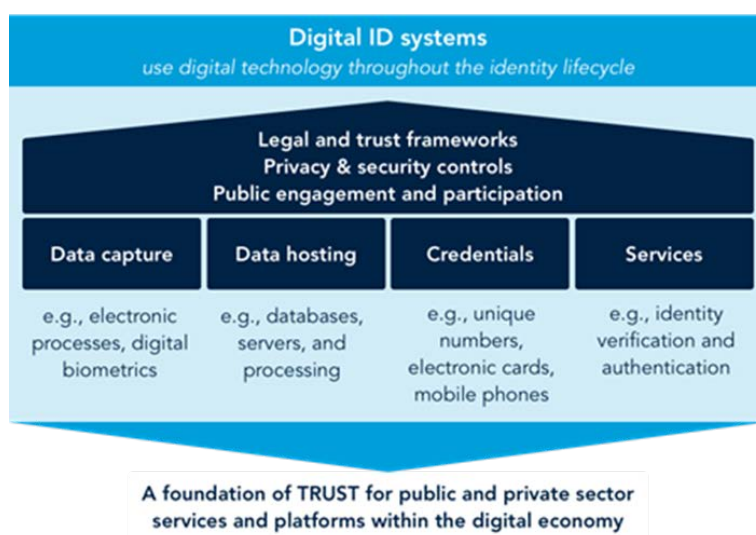
In addition to the direct effect on individuals, weak systems for verifying a person's identity and/or particular attributes about them—e.g., household information, income, occupation, etc.—also create administrative inefficiencies and opportunities for fraud and leakage. For example:

- A person may assume multiple identities (e.g., false or assumed names) when registering for benefits
- A head of household may inflate the size of their family by “borrowing” children from other households during registration
- When aid is in the form of guaranteed employment, a person who secures work may “outsource” that labor by selling it to another individual who performs the work in their place
- In long-term programs, the death of a beneficiary may not be reported in a timely fashion, allowing others to continue collecting the deceased's benefits if there is no ongoing authentication or credential checking
- People may collude with local officials to register fake or “ghost” beneficiaries to receive multiple or undeserved benefits if enrollment procedures or eligibility determinations can be manipulated
- Without secure authentication mechanisms, fraudsters may be able to collect benefits by impersonating beneficiaries with or without their knowledge

Source: Adapted from the *Digital Identity Toolkit*

These benefits can increase substantially with the adoption of digital technology—including electronic databases and credentials, biometric recognition for automated deduplication of identity records and/or authentication, mobile devices and applications, and interoperability platforms (see Figure 2)—that improve the accuracy of identity data and increase the efficiency of identity verification and authentication. However, while ID systems can create opportunities to further development goals, they also present multiple important challenges and risks.

Figure 2. Building blocks of digital ID systems



Source: Adapted from the *Digital Identity Toolkit*

Creating a good ID system presents risks and challenges, but there are common success factors

Building an ID system that meets developmental goals is a multifaceted challenge in any context, including mitigating potential risks to privacy and inclusivity, as well as system sustainability. In addition, developing countries face a unique set of challenges to implementing ID systems, particularly when digital. However, while no system is perfect, global experiences have also shown that there are common success factors that can help overcome these risks and challenges.

Risks of ID systems

The experiences of a broad range of countries at varying levels of development highlight four main risks to implementing new or upgraded ID systems:

- **Exclusion.** In contexts where people were previously able to prove their identities through alternate or informal means, the formalization of a new ID system and the tightening of identification requirements—e.g., making access to social programs or voting conditional on

a particular ID—risks further marginalizing vulnerable people who may not be covered by the system. Likewise, the failure of—or biases in—ID systems (e.g., failure of biometric authentication mechanisms, collecting data that is difficult for some people to provide, poor data quality, etc.) can lead to the exclusion of people from the ID system or accessing related services. Establishing a pro-developmental ID system therefore requires an exclusion risk assessment and explicit strategies to ensure access to identification for all, with particular attention to groups that are at higher risk of exclusion, such as remote and rural residents, the forcibly displaced, ethnic and linguistic minorities, people with disabilities, marginalized women and girls, and those with low connectivity or technical literacy. As part of the planning process, decision makers should also carefully consider the exclusion risks of formalizing or increasing identification/authentication requirements for different transactions.

- **Privacy and security violations.** Inherent in the capture, storage, and use of sensitive personal data are risks associated with privacy violations, data theft and misuse, identity fraud, and discrimination. The emergence of new technologies and the increased collection and use of personal data by state and non-state actors compounds these concerns and brings new threats from cybercrime and cyberattacks. ID systems therefore require strong legal and regulatory frameworks and a privacy-and-security-by-design approach to mitigate these risks and ensure data protection and user control. Cybersecurity of the system within a secure environment should be part of the a priori design. Furthermore, an assessment of risks to privacy and security should be incorporated into the planning process (e.g. a Data Protection Impact Assessment, cybersecurity penetration tests and audits) and continuously through the implementation of an ID system.
- **Vendor or technology lock-in.** Dependency on a specific technology or vendor can result in “lock-in” and/or dependency, increasing costs and reducing flexibility of the system to meet a country’s needs as they develop. This can occur, for example, through the adoption of a technology for which a limited number of suppliers are available, or contractual provisions in supply contracts or licensing agreements (e.g., for software) that restrict changes in technologies or vendors over time or may limit data ownership and access. Another cause of vendor dependency is when a vendor does not transfer knowledge or capacity to the government, which is a higher risk in poorly-designed public-private partnership and build-operate-transfer models. The risk of vendor and technology lock-in can be partially mitigated by the adoption of open, international standards and strong procurement practices that minimize unnecessary constraints in the choice of technology or supplier over unnecessarily long periods of time.
- **Unsuitable or unsustainable technology and design choices.** In many cases, countries have adopted high-cost systems that have failed to achieve development goals because they were unsuitable for the context or unsustainable in the medium or long term. For example, many countries have rolled out expensive multi-purpose smartcards for their national ID systems without relevant use cases or institutional structures to leverage this technology. Ensuring that systems provide a good return on investment and are sustainable over time requires a detailed appraisal of local context and capacity and robust procurement guidelines. Policymakers can also explore various models through which ID systems may produce cost savings for governments, as well as partnerships with the private sector that may reduce upfront costs. For example, linking an ID system with a strong CR system reduces the need for expensive, ad-hoc mass registration drives to update data. To

anticipate and control costs, a cost-benefit analysis of the system design should be completed during the planning process.

Challenges specific to low- and middle-income countries

In addition to these universal risks, many low- and middle-income countries face an additional set of challenges when implementing ID systems:

- **Weak civil registration systems.** Both CR and ID systems are crucial to ensuring legal identity for all (SDG 16.9) throughout a person's lifetime. In much of the developed world, ID systems are based on strong CR systems that have provided universal or near-universal coverage of life events, including births, marriages, and deaths (with certified medical causes) for generations. In many developing countries, however, CR systems have historically been weak. For example, approximately 60 percent of children under five-years old living in the least developed countries have never had their births registered (UNICEF 2017), while death registration rates are even lower. This can complicate the identity proofing process for ID systems—i.e., people may have no or only low-quality documentation of who they are, especially when a birth certificate is a requirement—and makes it difficult to automatically retire identities after a person has died.
- **Limited connectivity and other infrastructure.** In many countries, rural and remote areas lack reliable mobile and internet connectivity. This can create difficulties when implementing digital ID systems that require power and connectivity during enrollment (e.g., for data transfer or duplicate biometric enrollment check) and for authentication. Furthermore, core ICT infrastructure, such as secure data centers, may not exist. In addition, the general lack of infrastructure such as reliable roads in rural areas and regions with difficult terrain make certain households difficult to reach and can increase the time and cost of enrollment. If these issues are not addressed through technology choices and outreach, ID systems are likely to be exclusionary in low connectivity areas.
- **Lower literacy levels.** In low and middle-income countries, significant portions of the population may have lower literacy levels, both in terms of reading ability and the use of digital technology. This may translate into difficulties with enrollment, as well as the use of these systems for segments of the population who are likely to be among the most vulnerable. It also has implications for people's ability to provide informed consent to the collection and use of their data. As with low connectivity, illiteracy rates should be reflected in system design and implementation to minimize the potential for exclusion.
- **Lower government capacity and/or trust.** In certain countries, governments may have limited fiscal, technological, and administrative capacity to implement and/or regulate ID systems. Political instability and violent conflict may create or compound these difficulties in certain geographic areas or country-wide. In addition, past negative experiences may reduce people's confidence in the government and its ability to responsibly use and/or protect their personal data. While identity documents have been highly politicized in many countries—e.g., because of their link to certain rights such as voting—this may be exacerbated in contexts where the distribution of IDs can be more easily manipulated for political gain.

- **Poor procurement.** Low- and middle-income countries may have weak capacity and institutions to handle procurement and vendor contract management for an ID system, which is complex because of the wide-range of technologies available and different types of procurement that need to be completed. Further exacerbating this challenge are the tight deadlines that governments often impose for the introduction of an ID system, which puts pressure on agencies to reduce their planning time. The consequences of poor procurement processes and vendor contract management include failed procurements, delays (e.g. because of appeals), and vendor and technology lock-in.
- **Insufficient national cybersecurity capacity.** Low- and middle-income countries often have capacity gaps in their central cybersecurity agencies, which are needed to build a secure enabling environment for digital ID systems. Gaps can take the form of insufficient threat intelligence, breach monitoring and emergency response, sub-optimal hardware or software platforms, too few or insufficiently skilled cybersecurity analysts, weak cybercrime and cybersecurity legislation and weak cyber prosecution. The capacity of the central cybersecurity agency needs to be assessed for its ability to adequately support digital ID projects.

Success factors

Addressing these risks and challenges requires thoughtful design and thorough planning, along with sufficient technical, political, and financial resources. In addition, it requires the following factors, which are critical for successful ID systems:

- **Outcome and context-based design.** Key decisions regarding the design, rollout, and use of ID systems should be driven by the context, national goals, and people-centered perspectives, rather than by the technology itself. Technology choices should be based on a thorough analysis of the country's constraints and a clear understanding of how the system—including databases, credentials, etc.—will be used what its primary applications will be (e.g. improve targeting of social protection programs, improving financial inclusion, etc.). Practitioners must look beyond mass registration—which is only an input into an ID system—when they are designing an ID system and pay sufficient attention to its authentication functions and other uses, as this is what will drive the impact of an ID system. [Section II](#) of this Guide is designed to help practitioners walk through this design process.
- **Coordinated governance and sustained political commitment.** ID projects and systems are ambitious and involve an extremely high number of actors and stakeholders, including ministries, levels of government, private companies, and international organizations, civil society organizations, and more. Few projects touch every single person in a country like the introduction of a foundational ID system. For ID projects to succeed, they therefore require a high level of political commitment, a “whole of government approach,” and coordination to ensure a shared vision and a system that is useful to a variety of stakeholders. In addition, ID providing agencies require clear institutional and operational mandates and governance structures that provide enough capacity and resources to manage identification in the long-run.
- **Strong legal, regulatory, and operational frameworks.** ID systems require an enabling environment that adequately protects individual data and rights, minimizes security risks,

provides clear operational mandates and accountability, and ensures equality of access to identity documents and services. This includes primary and secondary legislation as well as internal operational guidelines, which should be updated to provide a holistic view of the collection, use, and management of personal data throughout the identity lifecycle, and is fit-for-purpose for the digital age.

- **A “privacy-and-security-by-design” approach.** Privacy and security should be built into the enabling environment and the functional and technical design of ID systems from the beginning—rather than as an afterthought. This includes adopting state-of-the-art legal, management, operational, and technical controls to ensure the protection of personal data from misuse, unauthorized disclosure, security breaches including cyberthreats and cyberattacks, and function creep. In addition, it includes building mechanisms to ensure user consent, control, and oversight of personal data.
- **Specific strategies and efforts to reduce the risk of exclusion during enrollment and authentication.** To ensure universal access to ID systems, practitioners must adopt a deliberate, ongoing strategy to ensure that no one is left behind. This may include updating laws and procedures to remove discriminatory measures, outreach efforts to specific groups that face higher barriers to obtaining ID or have concerns, exception-handling policies and procedures for those without ID that prevent exclusion to basic rights and services, and minimizing data collection and documentation requirements for registration.
- **Public engagement and consultation.** People are the subject and primary end-users of ID systems, yet these projects are often designed with little input from those they are designed to serve. Consultation during the planning phase and throughout implementation is crucial for understanding and mitigating barriers to access and designing ID systems that are user friendly and solve real problems. Conducting qualitative end-user research can help improve the design of ID systems from the perspectives of people (i.e. a bottom up rather than top down approach). Furthermore, intensive information campaigns are necessary to educate the public about registration, and—along with easily-accessible grievance redress mechanisms—are vital for reducing exclusion and improving trust in the system.
- **A holistic approach to CR and ID.** In order to (1) provide legal identity for all (SDG 16.9), (2) fulfill obligations for the continuous, permanent, compulsory and universal recording of vital events, and (3) ensure the accuracy and integrity of identity data overtime, countries should adopt a coordinated approach to simultaneously strengthen CR and ID systems and the linkages between these systems. In addition to independently investing in strengthening both systems, this could include interoperability and interfaces that allow for data exchange and/or queries, the assignment of a unique identity at birth from the ID system and through the CR system, and/or shared infrastructure and/or administration. Like any data exchanges between information systems, the linkages between CR and ID systems should be governed by relevant data protection laws and regulations. For example, a CR system collects more data for its statistical functions than are needed for identification, and thus only a limited amount of data needs to be shared.
- **Use of international standards.** Standards establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices with regard to the capture, storage, transmission, and use of identity data, as well as the format and features

of identity credentials and authentication protocols. They are therefore crucial at each stage of the identity lifecycle and help ensure that the building blocks of identity systems are interoperable and can meet desired performance targets. Furthermore, the use of international standards can help prevent vendor and technology lock-in by enabling the system to change its technology (e.g. ensuring data can be migrated and is compatible with different software), which is a key ingredient for operational and financial sustainability.

The ultimate purpose of this Guide is to help countries capitalize on these success factors and design successful ID systems that avoid the pitfalls described above.

Box 3. Additional ID4D publications

For more background on the potential developmental impact of ID, see the following publications (available at id4d.worldbank.org/research and described in [Section IV](#)):

- [G20 Digital Identity Onboarding](#)
- [The Role of Digital Identification for Healthcare](#)
- [The Role of Digital Identification in Agriculture](#)
- [Identification in the Context of Forced Displacement](#)
- [Identification for Development: Its Potential for Empowering Women and Girls](#)
- [The Role of Identification in Ending Child Marriage: Identification for Development](#)
- [The Role of Identification in the Post-2015 Development Agenda Digital Identity](#)
- The Role of Digital Identification in Education (*forthcoming*)

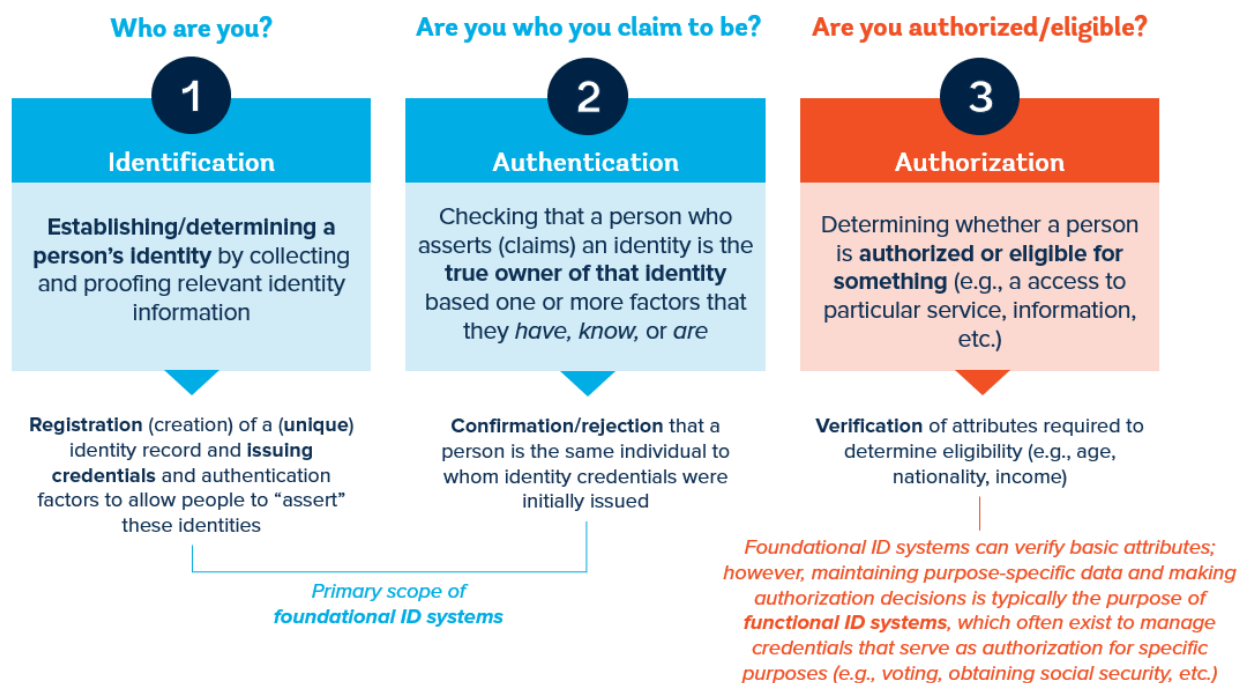
ID 101: BASIC CONCEPTS

“Identity” and “identification” can mean different things in different contexts. For the purposes of this Guide, **identity refers to the combination of characteristics or attributes that make a person unique in a given context**. While there are limitless personal attributes that are inherent to, chosen by, or ascribed to a person that make them unique, the particular attributes most relevant in this context include *core biographic data* (e.g., name, age, address) and certain *biometric features* (e.g., a facial image, fingerprints, iris scans).

See the [ID4D Glossary](#) in Section IV for a summary of identity-related terms used throughout this Guide.

ID systems collect and validate identity attributes in order to establish a person’s identity and provide proof of that identity in the form of a **credential** (e.g., unique ID number, card, certificate, mobile ID, etc.). These credentials can be used by the person through some method of **authentication** to “assert” or prove their identity to third, “**relying**” parties—e.g., government agencies, financial institutions, employers, etc.—that require some assurance of who they are.

Figure 3. The basic roles of ID systems



As summarized in Figure 3, **ID systems and personal attributes can help answer one or more of the following questions:**

1. “Who are you?”
2. “Are you who you claim to be?”
3. “Are you authorized or eligible for something?”

As described in [Section I. Why ID matters for development](#), these three questions are fundamental to service delivery and the fulfillment of rights and obligations. Both public and private sector institutions need to know who people are (question 1) and be able to trust that they are “really themselves” overtime—i.e., that no one has stolen or hacked their identity credentials (question 2)—as a part of many basic economic, social, political, and digital transactions. Furthermore, relying parties (e.g., service providers) may need to confirm—either during initial onboarding of a new beneficiary or client, or on an ongoing basis—that the person is eligible to access a particular right, service, information, or system functionality (question 3). Such determinations often require the ability to verify specific attributes about a person against a trusted source of information (e.g., a person’s age, income level, occupation, etc.).

In some cases, the same ID system used for identification and authentication may be able to provide the information needed for authorization or eligibility determination. In many other cases, however, relying parties must maintain or access additional information that is beyond the scope of the ID system itself. For example, a social service agency may rely on a person’s government-recognized digital ID to identify and authenticate a new beneficiary, ensuring that they really are the person that they claim to be. In order to determine whether the person is eligible for a specific safety net program, however, the agency may also need to verify a person’s income against a different trusted source of information (e.g., a tax register) to determine whether or not they are eligible for certain benefits.

Types of ID systems

The focus of this Guide is on ID systems that provide proof of legal identity that is often required for—or simplifies the process of—accessing basic rights, services, opportunities, and protections.

Historically, governments have operated a variety of ID systems to serve this and other purposes. Primarily, this includes *foundational ID systems*, such as civil registers, national IDs and population registers, which are created to provide identification to the general population for a wide variety of transactions. An ID system can be considered *legal* ID system to the extent that it enables a person to prove who they are using credentials recognized by law or regulation as proof of legal identity—i.e., most foundational ID systems (see Box 4).

In addition, governments have often created a variety of *functional ID systems* to manage identification, authentication, and authorization for specific sectors or use-cases, such as voting, taxation, social protection, travel, and more. In some countries—and particularly those that do not have a foundational ID system beyond civil registration—functional identity credentials are used as *de facto* proof of identity for purposes beyond their original scope. In the United States, for example, social security numbers and driver’s licenses in the United States are issues as proof of authorization for specific purposes but are used as general-purpose credentials. However, functional ID systems are typically not considered to be *legal* ID systems unless they are officially recognized as serving this purpose.

Box 4. Defining “proof of legal identity”

Proof of legal identity is defined as a credential, such as birth certificate, identity card or digital identity credential that is recognized as proof of legal identity under national law and in accordance with emerging international norms and principles.

Legal identity is defined as the basic characteristics of an individual’s identity. e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally-recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death.

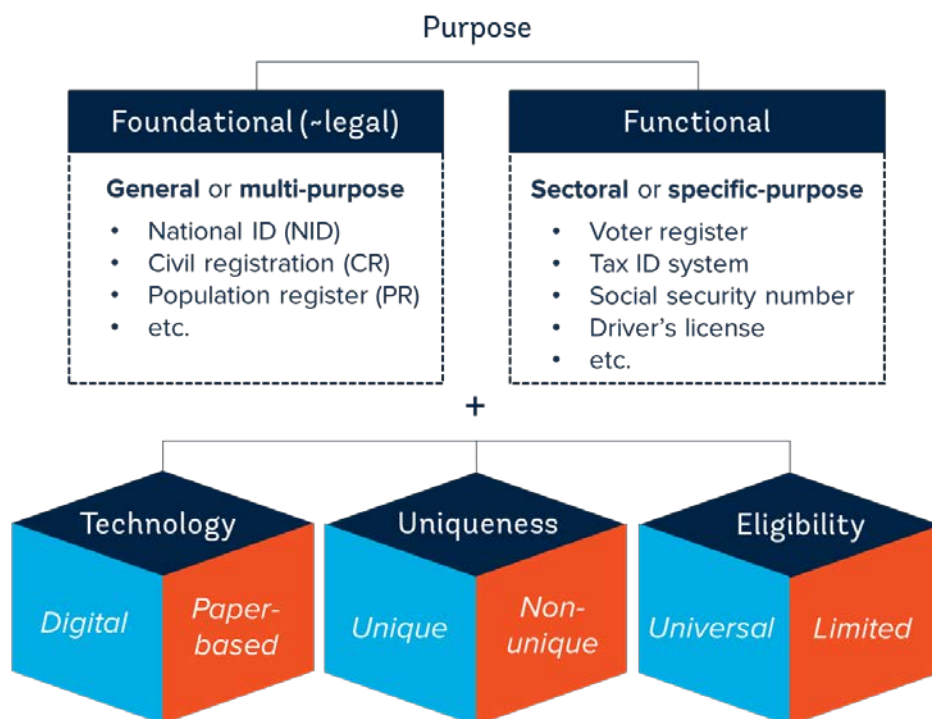
In the case of refugees, Member States are primarily responsible for issuing proof of legal identity, including identity papers. The issuance of proof of legal identity to refugees may also be administered by an internationally recognized and mandated authority (1951 Convention on the Status of Refugees Articles 25 and 27).

Source: United Nations Legal Identity Expert Group (LIEG) and World Bank Operational Definition of Legal Identity, <https://www.unhcr.org/en-us/1951-refugee-convention.html>.

As shown in Error! Not a valid bookmark self-reference., both foundational and functional ID systems vary along multiple dimensions, including:

- The technology they use;
- Whether they establish uniqueness; and
- Who they cover in the population.

Figure 4. Classification of government ID systems



In terms of technology, these ID systems can be *paper-based* or *digitized*. Digital ID systems are those that use digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication. Although the term “digital ID” often connotes identity credentials used for web-based or virtual transactions (e.g., for logging into an e-service portal), digital IDs can also be used for stronger in-person (and offline) authentication.

In addition, these ID systems may or may not uniquely identify individuals within a given population. Uniqueness typically means that (a) one person does not claim multiple identities within the system, and (b) each identity is only claimed by one person. In general, most foundational and functional ID systems are intended to be unique. However, some may have less reliable identity records due to a lack of deduplication, non-unique identifier generation (e.g., recycling ID numbers over time), or weak identity proofing procedures. In other cases, allowing for multiple registration may be a feature of the ID system functionality. For example, the same person can enroll multiple times in the UK’s Verify system, because its focus is on proof of identity, with any issues of uniqueness handled by the relying party, as described in Box 38.

Finally, these ID systems also vary based on the population that they are intended to cover. Because the purpose of foundational systems has been to provide broad (or universal, in the case of CR) coverage within the population, they are typically more inclusive in scope than functional systems, which—by their nature—are often limited to a certain subset of the population (e.g., people eligible to vote, beneficiaries of a cash transfer, people who have passed a driver’s test, etc.). In some cases, however, functional ID systems have relatively broad coverage because their program is intended to be universal (e.g., the US social security number). Similarly, not all foundational ID systems cover the entire population. For example, a country’s civil registry only covers vital events that occur within the territory, and therefore does not cover migrants or (in some cases) nationals born abroad. Similarly, some national ID systems only cover nationals, foreign residents with a valid visa, and/or people over age 18. In contrast other countries have implemented inclusive foundational ID systems that are accessible to all people within a territory or jurisdiction.

Within a given jurisdiction, there are normally many government and private-sector ID systems that together make up the *identity ecosystem*. As ID systems become digital, these ecosystems may be increasingly complex, with a wide range of identity models and actors with diverse responsibilities, interests, and priorities. The particular path that a country takes to develop a digital identity ecosystem will depend on a variety of factors, including which ID systems and assets already exist, and the identity-related needs of key stakeholders in both the public and private sectors.

Role of a foundational ID system

The focus of this Guide is on the design and implementation of *foundational, digital ID systems* that provide people with proof of legal identity. As shown in Figure 5, inclusive and trusted foundational ID systems can serve two important functions within the identity ecosystem and across a variety of sectors:

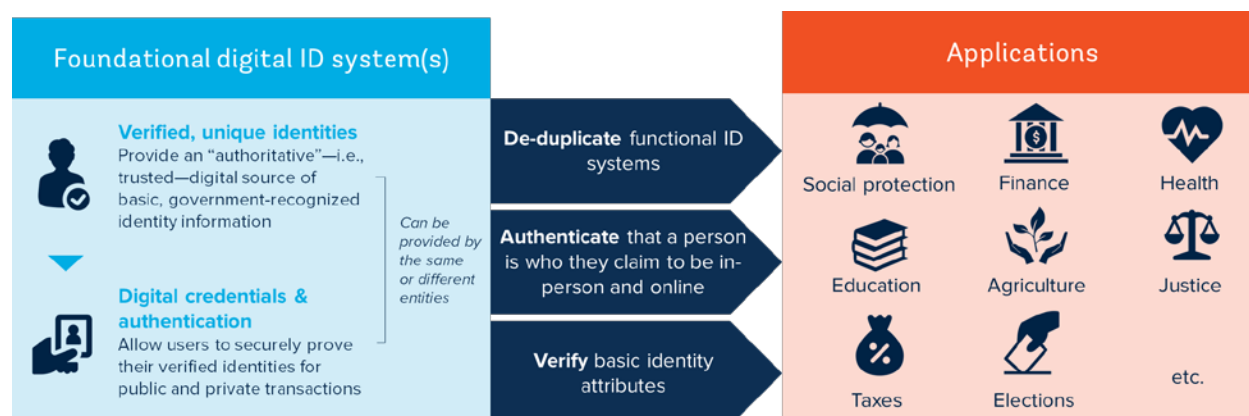
1. **Authoritative source(s) of basic identity information.** By creating a register of unique, verified identities, a foundational ID system can provide the basis for secure identity verification for government and private-sector users. In any country, having one or more trusted sources of basic identity information is vital to the integrity of the identity proofing

process for government functional ID systems and for private-sector ID providers and relying parties (e.g., financial institutions or MNOs conducting KYC). Beyond the verification of identity attributes themselves, a foundational system with unique identity records can also help deduplicate functional systems—e.g., a cash transfer register or public payroll—reducing opportunities for fraud and the need for redundant data collection by the foundational system (see *Public Sector Savings* paper).

2. **Credential and authentication provider.** In addition to establishing an authoritative source of identity information that can be leveraged by other systems, foundational ID systems can also provide credentials that allow people to authenticate their identities for a wide variety of purposes and sectors. As with verification, authentication can be a shared service provided to a variety of public and private sector users. When built as a platform that allows users to leverage the ID systems' credentials and authentication rather than building their own, this can help reduce costs for government agencies and private companies (See *Private Sector Savings* paper).

As described in more detail in the Introduction, having one or more interoperable foundational ID systems that serve these functions can improve access and service delivery across a variety of sectors, including health, education, social protection, financial inclusion, etc.

Figure 5. Potential role of a foundational ID system



Source: Adapted from *Digital Identity Toolkit*

In order further these development goals, however, foundational ID systems must be *inclusive*, and they must be *trusted*. In accordance with SDG 16.9 and the *Principles for Identification*, all people must have access to proof of their legal identity, no matter their age, nationality, or where they were born. CR systems are an important part of this infrastructure and provide the authoritative source of certain attributes as they were at the time of birth or death (i.e., at the moment births or deaths were registered) assuming that they were accurately recorded. Some of this information (e.g., name, legal guardians, and sex) could change over a person's lifetime, while other attributes (e.g., date and place of birth or death, and birth parent's identities) are immutable. However, CR systems are not dynamic registers of identity data, and—because they only cover events that occurred within the jurisdiction—they cannot be an authoritative source of information for people who were born elsewhere or who never had their vital events registered.

Providing legal identity for all therefore requires the strengthening of CR systems alongside—and in coordination with—the development of ID systems that can leverage and build on the CR while adding functionality (e.g., identity proofing, online verification and authentication services, portable credentials, etc.). In addition—and as enshrined in Principles 1 and 2, countries must ensure that everyone has access to foundational ID system, regardless of who they are. This requires a conscious and continuous efforts to remove or mitigate barriers to accessing proof of identity that are common among vulnerable populations.

In addition, foundational ID systems will only achieve the benefits described above when they are trusted—both by people and the institutions and companies that rely on them. Where people do not trust the provider of an ID system to manage and protect their data, they are unlikely to participate. Systems with low coverage have limited utility for governments or people and will necessitate parallel business processes to deal with people who are and are not covered. Similarly, where the data or credentials provided by an ID system are known or perceived to be inaccurate or susceptible to fraud or tampering, service providers will not be able to take this information at face value. Effective public engagement, robust legal frameworks, and a privacy-and-security-by-design approach are therefore fundamental to ensuring the overall success of the system.

New models for foundational ID in a digital world

In the past, most foundational (and functional) ID systems were paper-based and operated or managed entirely by governments. With the move toward digital technology throughout the identity lifecycle, however, we have begun to see new models of partnerships or trust frameworks between governments and the private sector to provide digital layers on top of existing legal ID systems that are recognized by the government for official online transactions. Typically, these systems leverage existing government-owned identity registers as authoritative sources of information to provide digital authentication and verification services for both official purposes and private sector applications.

A number of authors—notably ITU (2018) and WEF (2016)—have developed typologies to categorize these new digital ID ecosystem models, typically based on the role of the private sector in providing digital identities, and the structure of these arrangements (e.g., federation). For the purpose of this Guide, it is also important to distinguish an additional dimension beyond the number and type of digital ID (i.e., credential and authentication providers), which is the *type of authoritative source(s) these digital ID use for identity proofing*. Using these dimensions, we can classify various models used to provide people with *government-recognized* or legal identity in a digital form:

- **Centralized:** Under the centralized model, there is a *single provider* for a digital ID system recognized by the government as providing proof of legal identity.
 - In some cases, this may be the same entity that maintains the authoritative source register (e.g., a national ID or population register) on which the digital ID is based (e.g., **Belgium's eCard**, **Netherlands' DigiD**, **India's Aadhaar**, and many others).
 - In other cases—i.e., where there is no foundational ID system—the official digital ID may be provided by an entity that relies on *multiple* functional or lower-tiered government ID systems as authoritative sources for identity proofing (e.g., the current myGovID system in **Australia**).

- **Federated:** Under a federated model, multiple entities provide a government-recognized digital ID, coordinated or accredited through a trust framework or federation authority.
 - In some cases, these identity providers are public and/or private entities and that leverage a foundational ID system as their authoritative source (e.g., Bank ID in **Sweden**, **Norway**, and **Finland**, NemID in **Denmark**, **Belgium's Itsme®**)
 - In others, they draw from multiple functional systems as well as civil registers through a “broker” or federation authority (e.g., **GOV.UK Verify**, **Canada's SecureKey**).
- **Open-market:** Finally, countries could have multiple, regulated entities that provide government-recognized digital ID based on multiple functional IDs and or civil registers as authoritative sources of identity. In contrast to the federated system, however, these providers operate based on bilateral agreements with individual government agencies that provide online services rather than through a central or brokered scheme (e.g., **U.S.**).

In addition to the government-recognized forms of digital identity discussed above, countries may have a host of other digital ID systems maintained by public or (primarily) private sector entities for their internal use and for unofficial purposes. This might include, for example, private-sector-provided IDs that are **derived** directly from the government-recognized authoritative sources or digital IDs described above, issued after identity proofing based on non-governmental sources, or self-asserted (e.g., **social media**, **email accounts**, **commercial platforms**, etc.). In addition, there are emerging models of decentralized or distributed-ledger-based digital identity that seek to put people—rather than ID authorities, providers or relying parties—in control and at the center of identity transactions. However, distributed digital identity solutions typically rely on official data sources (i.e., foundational and/or functional government systems) to substantiate basic identity attributes in the first instance. To our knowledge, such models have not yet been accepted as legal proof of identity for use in official (online or in-person) transactions.

Importantly, different models of digital ID can exist within the same jurisdiction—in **Belgium**, for example, people can log-in to online government services using either the centrally-provided eCard, or the Itsme® digital ID (the first certified credential provider in an emerging federated scheme). This can improve people's control over their digital identities by offering them a choice of providers (and the ability to switch to more trusted or user-friendly services as needed).

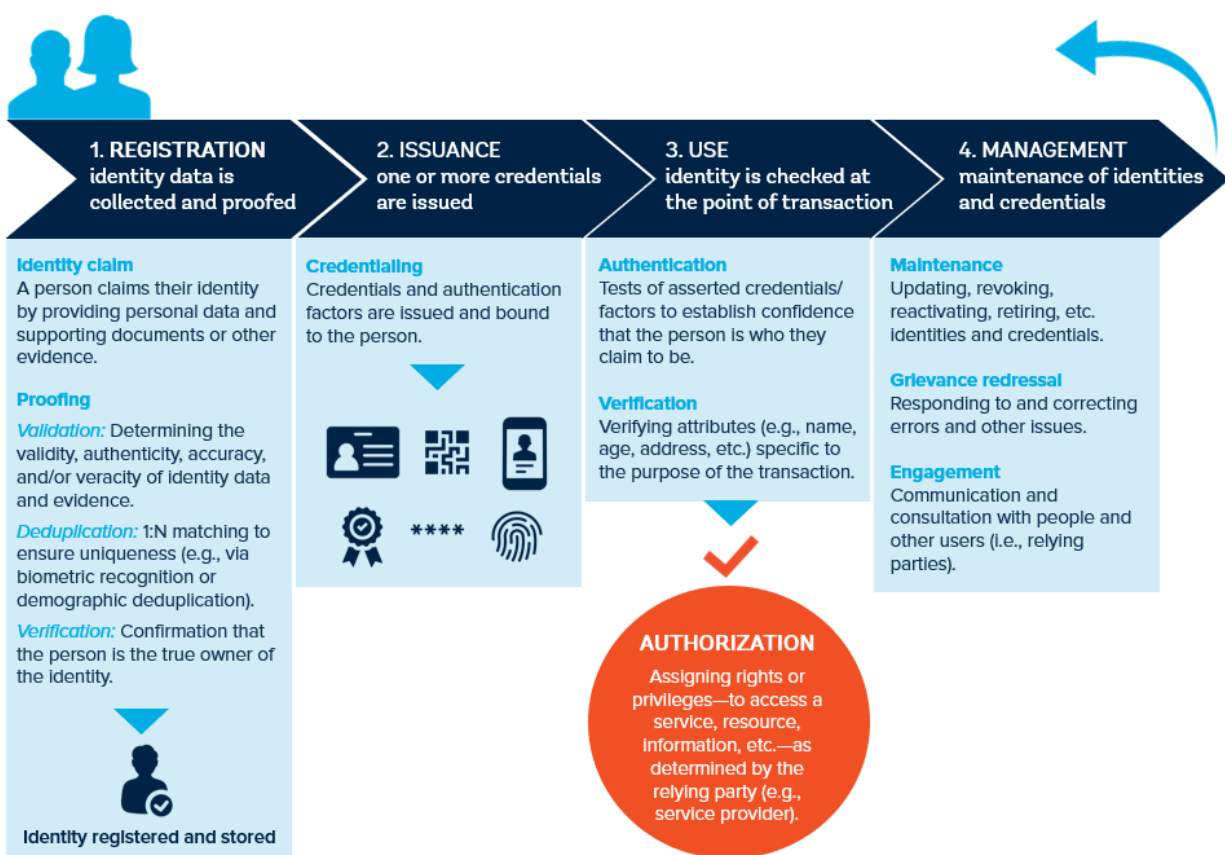
The ideal model of providing a digital, government-recognized ID system is very country-specific, and depends on the country's historical development, the trustworthiness of existing registers and other authoritative sources of identity information.

Identity lifecycle

In any ID system, the process of establishing a person's identity and then using this identity in later transactions involves multiple stages often referred to as the “**identity lifecycle**.” This lifecycle is vital to creating trust in a variety of transactions between people, identity providers, and public and private sector relying parties.

As the name implies, the identity lifecycle is not a one-time event (see Figure 6 below). Rather, it is a process that starts when a person first registers and their identity is created; continues with authentication of that identity and updates to their attributes and credentials over time; and ends when an identity record is retired or invalidated (e.g., after death, request for removal by the individual, or some other event). As discussed above—and in the section below on stakeholders and roles—the lifecycle may be completed by a single actor (e.g., an ID authority) for a given ID system, or may be split between multiple public and/or private sector actors (e.g., different registration authorities vs. credential and authentication providers).

Figure 6. Identity lifecycle



Source: Adapted from *Digital Identity: Public and Private Sector Cooperation* and *Technology Landscape for Digital Identification*

The technology and protocols used throughout the lifecycle—including for registration, credential issuance, authentication, and management—are critical for ensuring the inclusivity and trustworthiness of the system and its ability to facilitate authentication for different transactions at the appropriate “level of assurance.” Each stage is described briefly below.

Registration

The lifecycle begins when an individual first registers their identity, which involves two main processes:

- **Identity claim.** Registration begins with capturing and recording attributes from a person who “claims” a certain identity, such as biographic data (e.g., name, date of birth, gender, address, email) and biometric features (e.g., fingerprints, face, iris scan). It also may include the collection of meta-data about the time and location, location, and other details of the claim, which might be necessary for auditing purposes. During this process, people also typically provide supporting documentation or evidence to substantiate their claimed identity or—in the absence of such evidence—they may have their data vouched for by a trusted person, such as a local government official. Which attributes and evidence are captured during this phase, the methods and standards used to capture them, and the resulting data quality will have important implications for the inclusivity and trustworthiness of the identity, the speed of data collection, program cost, interoperability with other ID systems, and its utility for various stakeholders.
- **Identity proofing.** Once a person has claimed an identity, the data they provide is then validated. This involves checking the validity, authenticity, and accuracy of the supporting documents or evidence provided and confirming that the identity data is valid, current, and related to a real-life person. Identity proofing also commonly involves a deduplication process to ensure uniqueness based on biographic data and/or biometric recognition (e.g., in cases where there is no trusted source of identity information). In some cases, identity proofing also includes a process to verify that the applicant is the true owner of the claimed identity and evidence (e.g., through biometric verification or a visual comparison of the physical person to a photo on a previously issued ID card).

Issuance

After registration, the identity provider issues one or more credentials and/or authenticators—e.g., cards, certificates, PINs, etc.—that can be used by a person alone or in combination to prove or “assert” the identity that has just been created. For an ID to be considered digital, the credentials issued must store data electronically and/or be usable in a digital environment (e.g., being machine readable and/or usable on the internet). As with registration, the types of credentials issued, including their form factor and security features, have important implications for the robustness of the system to identity theft and fraud, as well as accessibility. In addition, the format of credentials such as cards is a major driver of the cost of ID systems.

Use

Once a person has been registered and credentialed, they can then **authenticate** or “prove” their identity when needed to access associated benefits and services. The authentication process can involve one or multiple factors—i.e., identity credentials and/or authenticators. For example, people may use a username and PIN to login to an e-government portal to pay their taxes or use their card and photo or fingerprint to prove their identity at a hospital.

Authentication factors fall into one of three categories (see Figure 7), including: (1) something you have (e.g., a physical card, mobile device, or digital cryptographic key), (2) something you know (e.g., a password, PIN, or answer to a secret question), or (3) something you are (e.g., your fingerprint or other biometry). Using multiple factors increases the level of assurance (i.e., security or trustworthiness) in a transaction.

Figure 7. Common authentication factors



Source: Adapted from *Digital Identity: Public and Private Sector Cooperation*

In addition to, or as part of the authentication processes, ID systems can also be used to **verify** specific attributes of a person—e.g., their name or age—in accordance with regulations on data sharing. This can be done using the credentials that a person presents (e.g., info stored on a card's chip or a barcode), and/or by querying the database directly.

Once a person has been authenticated and/or their information verified, the relying party (e.g., a service provider) may also undertake a separate (but sometimes automatic) process to determine whether a person is **authorized** to access different services or transactions or perform some certain actions based on this identity/attributes. For example, after successfully authenticating an applicant's identity, a government office may still need to decide whether the person is eligible to receive a particular cash transfer or type of pension. This often requires the verification of additional, sector-specific attributes (e.g., their income or occupation) against a different trusted source (e.g., a tax authority) outside of the ID provider.

Management

Throughout the lifecycle, identity providers manage identity data and credentials through a dynamic process. Importantly, this includes updating and re-proofing identity attributes that change over time—e.g., address, marital status, profession, facial image, etc.—as well as updating, renewing, revoking, or deactivating credentials. These updates can be subject to proofing (compared with accepting self-declared information), but strict requirements can act as a disincentive for people to keep their data up to date or may even exclude them from being able to update data (e.g. requiring proof of an address). Identity records may be retired if it is discovered that they were fraudulently created, after security breaches, or following an individual's death. Identity providers must also work to correct errors, address grievances, and continuously engage with the public and relying parties.

Stakeholders and roles

A variety of actors are typically involved in establishing, maintaining, and using an ID system throughout the identity lifecycle. In the context of government-recognized ID systems, important stakeholders include:

- **Individuals.** People are the center of ID systems. As both the subject of these systems and the end-users who use their identity to access rights and services, they have the right to know and exercise appropriate oversight over how their data is collected, used, stored, and shared. Understanding and responding to people's ID-related needs and concerns, protecting their privacy and personal data, and ensuring their agency throughout the identity lifecycle must be the starting point for building an ID system capable of furthering development goals.
- **Governments.** Government agencies—e.g., ID authorities, civil registrars, Ministries of ICT, Interior or Justice, etc.—are often the primary providers of foundational ID systems. In addition, other government agencies—e.g., Ministries of Social Protection, Health, Education, Justice, Tax, Customs, election administration, etc.—either rely on these foundational systems to interact with people and/or are themselves providers of functional ID systems. Finally, other government bodies play a regulatory role, provide oversight for ID systems, and may also be involved in implementing specific components or setting standards for technology and data formats. For instance, national cybersecurity agencies help ID agencies reduce cybersecurity risks and effectively respond to breaches, and Ministries of ICT may provide infrastructure or shared services, such as a datacenter, government cloud, or public key infrastructure (PKI).
- **Private sector.** Private companies are developers, innovators, and suppliers of most ID system components and infrastructure. In addition, private companies may also be ID providers themselves, either as part of their core business (e.g., as part of federated or decentralized digital authentication models) or to identify and authenticate customers for other services, such as (e.g., financial service providers and mobile operators). In addition, many private companies rely on government ID systems to identify their customers (e.g. requiring government-issued credentials to open bank accounts, register SIM cards, or create credit reporting systems). Governments have also partnered with private companies to deliver forms of digital ID, such as mobile identity and digital authentication platforms, or to perform specific roles within a government-provided ID system (e.g., data collection during registration).
- **Civil society.** NGO, community-based organizations, and other local groups are important partners for generating demand for ID and assisting people in obtaining the proof of identity they need to fully engage in economic, political, and social life. For more on this topic, see the "Community-Based Practitioner's Guide on Documenting Citizenship and Other Forms of Legal Identity" (*Open Society Justice Initiative and Namati 2018*), which provides a toolkit for community-based justice actors to assist people in obtaining proof of legal identity. Civil society actors are also important potential partners and sources of critical feedback on the planning and implementation of ID systems.

- **International organizations and development partners.** Development and humanitarian agencies may provide support for ID systems in the form of funding and technical assistance or be involved in establishing ID systems themselves to administer programs. For asylum seekers and refugees, for example, the 1951 Convention on the Status of Refugees (articles 25 and 27) provides that host States are responsible for registration, refugee status determination and providing IDs. However, in some cases, host States may not have the capacity or willingness to do so, and UNHCR may take on this responsibility in partnership with the host State and in line with its mandate established in international law. Other international bodies—e.g., the International Standards Organization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU), International Civil Aviation Organization (ICAO)—are also involved in setting standards related to identity management.

Each of these stakeholders can play various roles within the identity ecosystem, as described in Table 1.

Table 1. ID Stakeholders, roles, and objectives

Role	Stakeholders	Core Activities	Primary Goals
“End-users” Subjects of the ID system	People Residents, citizens, beneficiaries, customers, etc.	<ul style="list-style-type: none"> ▪ Register in ID system ▪ Use credentials and proof of ID to access rights and services ▪ Update data as needed ▪ Exercise control and oversight over their data 	<ul style="list-style-type: none"> ▪ Accessibility ▪ User-friendliness and control ▪ Transparency and consent regarding data usage ▪ Privacy & data protection
“ID providers” Issue and manage identities <i>(Note: the term ID provider can comprise many separate roles; see Section III. Administration > Roles and Responsibilities for a more detailed discussion)</i>	Government agencies <i>Foundational:</i> ID authorities, civil registrars, etc. <i>Functional:</i> electoral commission; social protection, health ministries; tax authorities, etc. Private companies PPP partners, mobile operators, financial service providers, online commercial platforms, private health providers, credit rating agencies, etc. International organizations UNHCR, WFP, etc.	<ul style="list-style-type: none"> ▪ Register people in the ID system ▪ Issue and manage credentials ▪ Manage and update identity information ▪ Provide authentication/verification services at different levels of assurance ▪ Raise awareness, conduct public consultations, and redress grievances 	<ul style="list-style-type: none"> ▪ Create accurate, trusted identities ▪ Deliver services efficiently and effectively ▪ Protect data against misuse and breaches ▪ Prevent fraud ▪ Reduce operating costs

Role	Stakeholders	Core Activities	Primary Goals
“Relying parties” Rely on ID systems provided by others to identify/verify/authenticate end users	Government agencies Passport office, electoral commission, tax authorities, social protection agency, etc. Private companies Mobile network operators, financial service providers, online commercial platforms, private health providers, credit rating agencies, etc.	<ul style="list-style-type: none"> Use platforms, credentials, and services of ID providers to authenticate and/or verify the identity of end-users Authorize people to access specific rights or services 	<ul style="list-style-type: none"> Identify and authenticate people with appropriate level of assurance for transaction Deliver services efficiently and effectively Prevent fraud Reduce operating costs
“Enablers” Support the development, implementation, and oversight of the ID system	Regulatory bodies Government oversight and enforcement agencies	<ul style="list-style-type: none"> Promulgate and enforce regulations and trust frameworks related to ID 	<ul style="list-style-type: none"> Data protection and privacy Consistent identity management Accountability
	Standard setting bodies and trust frameworks Government and international organizations, private identity organizations and associations	<ul style="list-style-type: none"> Provide technical and data standards Build trust Support information security and cybersecurity 	<ul style="list-style-type: none"> Build trusted ID systems that are vendor and technology neutral Facilitate interoperability Establish trust between identity stakeholders
	Development and local partners Donor agencies, NGOs, community-based organizations	<ul style="list-style-type: none"> Provide funding and technical assistance for ID system design and implementation Assist people with accessing and using ID systems and related services Advocate for inclusive and trusted ID systems 	<ul style="list-style-type: none"> Support client goals Build local capacity Ensure accountability to users

Source: Adapted from *Digital Identity Toolkit* and *Digital Identity: Public and Private Sector Cooperation*

SECTION II. Designing an ID System

 DESIGNING an ID SYSTEM	 Principles <i>Principles on Identification for Sustainable Development provide high-level guidance</i>	 Planning Roadmap Steps to evaluate the country context, costs, benefits, and risks related to planned decisions	 Key Decisions Summary of big-picture design decisions to take before beginning procurement	 Procurement Best-practices and basic checklist to inform procurement
--	---	--	---	---

This section provides an overview of the planning process for designing an ID system, beginning with the **Principles on Identification** that underpin inclusive and trusted ID systems. It then presents a **planning roadmap** to guide practitioners through various exercises needed to understand gaps in the current ID system, identify goals for the future and country-specific constraints, and assess the costs, benefits and risks of particular design choices. Next, it summarizes the **key, high-level design decisions** that need to be made early in the planning process and concludes with **guidance on procurement**.

Contents:

- [Principles on Identification](#)
- [Planning Roadmap](#)
- [Key Decisions](#)
- [Procurement](#)

There is no one-size-fits-all solution for creating a foundational ID system that is inclusive and trusted. Instead, governments and other stakeholders must undertake an in-depth planning process to ensure that the design and implementation of a foundational ID system is appropriate to the country context and fit-for-purpose to achieve national priorities while respecting people's inalienable rights. This planning process should be informed by international good practices, reflect local needs, goals, and context, and begin the public and stakeholder consultations that should continue throughout ID system implementation.

Importantly, planning should begin with *high-level policy and design* decisions, which are needed to inform the development of core policies, laws, and regulations and to eventually complete technical specifications and procurement. Conversely, ID projects that begin with technical specifications—e.g., the desire for a particular credential or other technology—are less likely to succeed as they are driven by supply and not necessarily by demand. A foundational ID system is not an end in itself; it must be motivated by potential impacts (e.g., increasing inclusion and access to services, reducing fraud, etc.) and the expressed needs of people and other system users. This requires a paradigm shift from ID systems being systems of control or knowledge to platforms for service delivery, digital development, and empowerment. While this requires new thinking and business process re-engineering on the part of identity providers and relying parties, reconceiving identity as a user-centric platform will ultimately benefit people, governments, and the private sector.

This section provides a series of content to help navigate the planning and design process, including:

- **Principles.** An overview of the Principles on Identification for Sustainable Development, which provide a high-level guiding framework of good practices related to system inclusion, design, and governance. These Principles have been endorsed by 25 organizations—including UN agencies, donors, private sector associations, and research institutions—and should serve as a touchstone for any ID project.
- **Planning Roadmap.** In order to begin designing an ID system, practitioners must first identify and consider important country-specific factors, including the status quo of ID assets, stakeholders, coverage, quality, and legal frameworks; specific goals for the ID system; constraints such as existing ICT infrastructure, levels of development and connectivity, and other social, political, and economic considerations; fiscal costs and benefits of design-choices; and potential risks related to privacy and exclusion. This section summarizes important decision factors and presents various ID4D tools to assist in this process.
- **Key Decisions.** This section provides overview of key decisions that practitioners must make regarding the functional design of the ID system, which are needed to inform legal and regulatory frameworks and to eventually develop more detailed technical specifications needed for procurement. These decisions should be informed by the detailed assessments undertaken as part of the planning roadmap as well as more in-depth technical information provided in [Section III](#).
- **Procurement.** Once initial planning is complete and key decisions have been made, the Guide presents a checklist and good practices to assist countries with the procurement process.

1. PRINCIPLES

There are certain high-level standards that practitioners should follow to ensure that ID systems are inclusive, trusted, and useful for people, governments, and the private sector. This includes the ten Principles on Identification for Sustainable Development, which were developed through a series of stakeholder consultations and have been endorsed by 25 international organizations, associations, and development partners (see Table 2).



Table 2. Principles on Identification for Sustainable Development

PRINCIPLES	
INCLUSION: UNIVERSAL COVERAGE AND ACCESSIBILITY	<ol style="list-style-type: none"> 1. Ensuring universal coverage for individuals from birth to death, free from discrimination. 2. Removing barriers to access and usage and disparities in the availability of information and technology.
DESIGN: ROBUST, SECURE, RESPONSIVE AND SUSTAINABLE	<ol style="list-style-type: none"> 3. Establishing a robust—unique, secure, and accurate—identity. 4. Creating a platform that is interoperable and responsive to the needs of various users. 5. Using open standards and ensuring vendor and technology neutrality. 6. Protecting user privacy and control through system design 7. Planning for financial and operational sustainability without compromising accessibility
GOVERNANCE: BUILDING TRUST BY PROTECTING PRIVACY AND USER RIGHTS	<ol style="list-style-type: none"> 8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework. 9. Establishing clear institutional mandates and accountability. 10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

Source: *Principles on Identification for Sustainable Development*

The Principles are organized according to three pillars—inclusion, design, and governance—as summarized below.

Pillar 1: Inclusion

The first two principles are intended to ensure that no one is left behind by ID systems, in support of SDG 16.9: “By 2030, provide legal identity for all, including birth registration” (see <https://sustainabledevelopment.un.org/sdg16>).

Principle 1. Ensuring universal coverage for individuals from birth to death, free from discrimination.

The universal coverage Principle requires countries to **fulfill their obligations to provide legal identification to all residents—not just citizens—from birth to death**, as set out in international law and conventions and their own legislative frameworks. This includes the **commitment to universal birth registration** for those born on in their territory or jurisdiction and, in appropriate circumstances, linking civil registration and ID systems, which is an essential part of ensuring the accuracy and sustainability of ID systems.

In addition, ID systems should be **free from discrimination**, both in terms of who has access and how they are used. This requires practitioners to identify and mitigate legal, procedural, and social barriers to enroll in and use ID systems, with special attention to poor people and groups who may be at risk of exclusion for cultural, political or other reasons (such as women and gender minorities, children, rural populations, ethnic minorities, linguistic and religious groups, persons with disabilities, migrants, the forcibly displaced, and stateless persons). Furthermore, ID systems and identity data should not be used as a tool for discrimination, persecution, or to infringe on individual or collective rights.

Principle 2. Removing barriers to access and usage and disparities in the availability of information and technology

To ensure universality, Principle 2 calls for the **elimination of barriers to access and use ID**. This includes removing or reducing direct and indirect cost for identification. Civil registration and first birth and death certificates should be free of charge, as should the initial issue of any identity credential that is mandatory—*de jure* or *de facto*—to possess or to access basic rights and services. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. Consideration should be given to subsidizing or waiving application or service fees for poor and vulnerable persons. The indirect costs of obtaining identification—including fees for supporting documents, travel costs, and cumbersome administrative procedures—should also be minimized. For example, ID-related services should be available online and should routinely visit remote communities.

Furthermore, practitioners should **mitigate information disparities and the digital divide** by working to ensure user literacy regarding ID systems, fostering a culture of understanding and trust, and reducing information asymmetries that might prevent individuals from accessing identification-related services or benefits. With the rise of digital systems, no one should be denied identification or associated services because they lack mobile or internet connectivity or digital literacy. Stakeholders should work together to ensure both online and offline infrastructure can be extended to provide “last-mile” access and connectivity, particularly for those in rural and remote areas.

Pillar 2: Design

In addition to providing universal coverage, ID systems should be **robust** to fraud and error, **useful** for a variety of stakeholders, and **sustainable** over time. ID system design must also **protect user**

privacy and adopt **open standards** to facilitate innovation, interoperability, and vendor and technology neutrality.

Principle 3. Establishing a robust—unique, secure, and accurate—identity.

Principle 3 highlights that **accurate**, up-to-date information is essential for the trustworthiness of any identification database and credentials used for authentication. Foundational ID systems should provide a **unique identity** that is verifiable over the course of a person's life, from birth to death—i.e., within a given foundational ID system, each person should have only one identity, and no two people should have the same identity. In addition, ID systems must have safeguards against tampering (alteration or other unauthorized changes to data or credentials), identity theft, data theft and misuse, cybercrime and other threats occurring throughout the identity lifecycle.

Principle 4. Creating a platform that is interoperable and responsive to the needs of various users.

Principle 4 highlights the need for identification and authentication services to be **flexible, scalable**, and **meet the needs and concerns of people (end-users)** and **relying parties** (e.g., public agencies and private companies). To ensure that identity-related systems and services meet specific user needs, practitioners should engage the public and important stakeholders throughout planning and implementation. The value of ID systems to relying parties is highly dependent on their interoperability with multiple entities, both within a country and across borders. Domestically, this includes the ability of different databases or registries (e.g., national ID and civil registration systems) to communicate with each other, exchange data, and facilitate identity queries in a timely and low-cost manner (e.g., via open APIs), subject to appropriate privacy and security safeguards. It also includes **interoperability across borders** to facilitate mutual recognition of physical or digital IDs issued by one country in other countries, which can increase trade and enable safe and orderly migration.

Principle 5. Using open standards and ensuring vendor and technology neutrality.

Principle 5 further emphasizes the need for **vendor and technology neutrality** to increase flexibility and avoid system design that is not fit for purpose or suitable to meet policy and development objectives. This requires robust procurement guidelines to facilitate competition and innovation and prevent possible technology and vendor “lock-in,” which can increase costs and reduce flexibility to accommodate changes over time. In addition, open design principles enable market-based competition and innovation. They are essential for greater efficiency and improved functionality of identification systems, and for interoperability. Similarly, open APIs also support efficient data exchange and portability by ensuring that a component of the ID system can be replaced with minimal disruption.

Principle 6. Protecting user privacy and control through system design.

In addition to architecture that is responsive and flexible, Principle 6 emphasizes that ID systems must protect people's privacy and control over their data through system design. Designing with people's privacy in mind means that **no action should be required on the part of the individual to protect his or her personal data**. Information should be protected from improper and unauthorized use by default, through both technical standards and preventative business practices. These measures should be complemented by a strong legal framework (as emphasized in Principle 8).

For example, data collected and used for identification and authentication should be **fit for purpose, proportional to the use case**, and managed in accordance with global norms for data protection, such as the OECD's Fair Information Practices (FIPs) (see <http://oecdprivacy.org/>) and with reference to emerging international good practices, such as the European Union's General Data Protection Regulation (GDPR). Authentication protocols should only provide "yes or no" confirmation of a claimed identity or—if mandated by law such as Anti-Money Laundering regulations (AML) related to Customer Due Diligence (CDD) or Know Your Customer (KYC)—only disclose the minimal data necessary for the transaction. The method of authentication should reflect an assessment of the level of risk in the transactions and can be based on recognized international standards and frameworks for levels of assurance. Credentials and numbering systems **should not unnecessarily contain or disclose sensitive personal information** (e.g., use randomized numbers without any logic).

Principle 7. Planning for financial and operational sustainability without compromising accessibility

Principle 7 recognizes the importance of designing systems that are **financially and operationally sustainable** while still maintaining accessibility for people and relying parties. This may involve different business models including reasonable and appropriate service fees for identity verification, offering enhanced or expedited services to users, carefully designed and managed public-private partnerships (PPPs), recuperating costs through efficiency and productivity gains and reduced leakages, and other funding sources. It also includes potential linkages between civil registration and ID systems, which can ensure the integrity of the system over time without the need for costly re-registration efforts by notifying the system of life events (e.g., deaths) automatically.

Pillar 3: Governance

The final group of principles addresses how ID systems should be governed to protect **user privacy and rights, system security**, and **clear accountability** and **oversight**.

Principle 8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.

Principle 8 sets out the requirements for a comprehensive legal framework: **ID systems must be underpinned by policies, laws and regulations that promote trust in the system, ensure data privacy and security, mitigate abuse such as unauthorized surveillance in violation of due process, and ensure provider accountability.**

This typically includes an enabling law and regulations for the ID system itself as well as laws and regulations on data protection, digital or e-government, electronic transactions and commerce, AML, civil registration, cybersecurity and cybercrime, functional ID systems, and freedom of information, among others. The enabling law and regulations for an ID system should clearly describe the purpose of the ID system, the ID system's components, roles and responsibilities of different stakeholders, how and what data is to be collected, liability and recourse for ID holders and relying parties, the circumstances in which data can be shared, correction of inaccurate data attributes, and how inclusion and non-discrimination will be maintained. Laws and regulations on data protection and privacy should include oversight from an independent body (e.g. a national privacy commission) with appropriate powers and should protect ID holders against inappropriate access and use of their data by third parties for commercial surveillance or profiling without informed consent or lawful purpose. At the same time, these frameworks should not stifle competition, innovation, or investment and can include regulatory and self-regulatory features.

In addition, **the ID-related laws, regulations, and policies should enable people with genuine choice and control over the use of their data**, including the ability to selectively disclose the attributes that they want. Users should be given simple means to have inaccurate data corrected free of charge and to know what data is being held about them. Personal information should not be used for secondary, unconnected purposes without the user's informed consent, unless otherwise required under the law. ID providers should be transparent about identity management, develop appropriate resources to raise users' awareness of how their data will be used, and provide them with tools to manage their privacy. ID providers should ensure that the initial process to correct errors is administrative rather than judicial in order to increase speed of resolution and reduce costs. Data sharing arrangements should also be transparent, fully documented, and serve the best or vital interests of the individual(s) concerned.

Principle 9. Establishing clear institutional mandates and accountability.

Principle 9 highlights the need for institutional mandates and accountability in the governance of ID systems. Ecosystem-wide trust frameworks must establish and regulate governance arrangements for ID systems. This should include specifying the terms and conditions governing the institutional relations among participating parties, so that the rights and responsibilities of each are clear to all. There should be clear **accountability and transparency** around the roles and responsibilities of identification system providers.

Principle 10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances

Finally, Principle 10 emphasizes that the ID system should include clear arrangements for the **oversight of these legal and regulatory requirements**. The use of ID systems should be **independently monitored** (for efficiency, transparency, exclusion, misuse, etc.) to ensure that all stakeholders appropriately use identification systems to fulfill their intended purposes, monitor and respond to potential data breaches, and receive individual complaints or concerns regarding the processing of personal data. Furthermore, disputes regarding identification and the use of personal data that are not satisfactorily resolved by the providers—for example, refusal to register a person or to correct data, or an unfavorable determination of a person’s legal status—should be subject to **rapid and low-cost review by independent administrative and judicial authorities** with authority to provide suitable redress.

2. PLANNING ROADMAP



To ensure that ID systems meet national goals and reflect local needs and constraints, practitioners should adopt an **outcome-based and context-specific approach to making policy and design decisions**. Specifically, this should include an analysis of the following:

- **Status quo**—What ID systems are currently operating within the country and what are their strengths and weaknesses?
- **Vision**—What are the main goals of creating a new (or improving an old) ID system, and how will it benefit people, the government, and the private sector?
- **Constraints**—What are the anticipated obstacles or challenges to the planned ID system?
- **Costs and benefits**—What are the anticipated financial impacts of the planned ID system?
- **Risks**—What are the potential risks of planned ID systems related to privacy, security, and exclusion?

The remainder of this section guides practitioners through each of these topics and references **core ID4D planning tools** to assist with these exercises, including:

- *ID4D Diagnostic*—Guidelines for evaluating the ID ecosystem and strengths and weaknesses of existing ID systems.
- *ID-Enabling Environment Assessment (IDEAA)*—Checklist and guidelines for evaluating the legal, regulatory, and policy framework for ID.
- *Costing model*—Spreadsheet and guidance note for estimating the price tag of ID systems based on country characteristics and design choices.

- *Public Sector Savings*—Framework for assessing opportunities for fiscal savings in the public sector
- *Private Sector Savings*—Discussion of potential channels for private-sector savings and revenue generation from ID system.
- *End-user research toolkit (pre-publication)*—Toolkit for implementing qualitative end-user research to understand people’s needs, barriers, and concerns regarding identification.
- *Procurement checklist (pre-publication)*—Detailed checklist and guidelines for issuing and evaluating RFPs for ID systems.

Understand the Status Quo

An analysis of the current identity landscape is a valuable exercise for countries planning new identification systems and those hoping to optimize existing systems. To maximize the utility of identification in the medium- and long-term, it is important to first take a holistic view of existing ID systems and stakeholders within the identity ecosystem and assess their strengths and weaknesses, particularly regarding system coverage, quality, and the enabling legal framework.

ID4D has developed multiple tools to assist in this type of exercise, including an *ID4D Diagnostic* for an ecosystem-wide overview, and the *ID Enabling Environment Assessment (IDEEA)* for a comprehensive analysis of the policies, laws, and regulations that enable the ID system and provide key safeguards. These tools are flexible and designed to be adapted based on the country context.

In addition to desk reviews and consultations with government stakeholders, diagnostics of the status quo should also include the perspectives of end-users as well as various government and private-sector institutions who rely on these systems. In particular, it is recommended that countries consult with individuals to understand their particular experiences and challenges with the existing ID system (see *forthcoming toolkit for end-user research*).

1. Take stock of the identity ecosystem and stakeholders

The current landscape of ID systems—aka, the identity ecosystem—has important implications for the design of future systems or reforms. To begin, countries should make a full accounting of existing registries and credentials, as well as the agencies that provide them and their core users. As shown in Table 3, this should include:

- Foundational registries and credentials
- Functional registries and credentials used in various sectors (e.g., social protection, voter registration, tax administration, passports, driver’s licenses, etc.)
- Non-governmental ID systems provided by other actors
- Current ID providers and their roles in each of these systems
- Supporting and enabling agencies

Table 3. Identity ecosystem stock-taking

System	Providers	Users	Supporters/Enablers
Foundational	e.g.,		

System	Providers	Users	Supporters/Enablers
<ul style="list-style-type: none"> National ID Civil register Population register, etc. 	<ul style="list-style-type: none"> Ministry of Interior Ministry of Justice Ministry of Health Local governments, etc. 		<ul style="list-style-type: none"> Regulator/oversight body Ministry of finance Ministry in charge of Digital Government Ministry in charge of digital infrastructure, including broadband connectivity Agency in charge of Cybersecurity technology Civil society Donors and other development partners
Functional <ul style="list-style-type: none"> Voter registry Social assistance registries Taxpayer registry Passport Driver's license Land registry Property registry, etc. 	e.g., <ul style="list-style-type: none"> Electoral commission Ministry of Social Affairs Revenue Department Immigration Department Transportation Department Ministry of Interior Etc. 	<ul style="list-style-type: none"> Other agencies Private sector Donors Individuals 	
Non-Governmental <ul style="list-style-type: none"> Financial sector IDs SIM card registry Credit registry Donor program registries, etc. 	e.g., <ul style="list-style-type: none"> Banks Mobile operators Credit agencies Donors and Int'l Organizations 		

Source: *ID4D Diagnostic Guidelines*

In addition to identifying the various stakeholders who should be involved in the planning process, the characteristics of the existing identity ecosystem will be important inputs into key decisions. This includes the **number of ID systems**, as well as the **capacity of various stakeholders**. To effectively manage an ID system, identity providers must have sufficient **human, technical, and fiscal resources**, as well as substantial **political support** within the government and from other relevant stakeholders.

Table 4. Design implications of existing ID ecosystem and stakeholders

Ecosystem characteristic	Implications for Key Decisions
Existence of core foundational systems (e.g., civil registers and national IDs)	<p>Administration: In a “greenfield” project where there is no national ID system and/or the system is very weak, countries can either assign the new ID system to an existing agency, or create a new agency to implement the new ID system. Where countries already have foundational systems, it may be less desirable, or more politically infeasible to create new agencies for this purpose. Countries may wish to add the responsibility for an ID system to the agency responsible for civil registration.</p> <p>Registration: Where foundational ID systems exist but countries wish to improve or extend these systems to new populations, they must choose whether to leverage existing hardware, software, and/or data (e.g., initializing the new ID system by cleaning and updating old data, or using the old system as a source of evidence identity proofing in the new</p>

Ecosystem characteristic	Implications for Key Decisions
	<p>system), or whether to invest in new systems and collect data from scratch. These choices should be heavily informed by the coverage and quality of these systems, described below.</p> <p>Credentials and Authentication: Where there are strong foundational ID systems with non-digital credentials (e.g., a legacy paper national ID card), countries can consider providing digital ID credentials centrally (i.e., by the foundational ID providers) or through a partnership or federated arrangement with other public and private sector entities.</p>
Number of functional ID databases and credentials	<p>Interoperability: Where there are already many operational ID systems for different sectors—e.g., tax, social protection, voting, etc.—countries can consider different options for integration and/or interoperability depending on the level of quality and trust in these systems.</p>
Resource deficits for existing ID authority, in terms of staff or financing, or unclear or overlapping mandates with other entities that limit capacity	<p>Legal Framework: Determine if updates are needed to the legal framework in order to better empower the ID authority and/or to clarify responsibilities.</p> <p>Administration: Consider creating new, autonomous agency to manage the ID system, new business models, and/or partnerships with other government agencies or with the private sector to fulfill some roles and responsibilities, such as for registration.</p>

2. Determine coverage and gaps in the existing systems

In addition to looking at the overall composition of the identity ecosystem, an assessment of the status quo should include an evaluation of the rate and gaps in coverage of foundational systems and key functional systems. This involves an examination not only of the *number* of people covered, but also an analysis of *specific groups* that may be disproportionately excluded from existing ID systems. In many countries, for example, we often see differential rates in coverage for the following groups (and their intersections):

- Women and girls
- Orphans and vulnerable children
- Poor people
- Rural dwellers
- Ethnolinguistic minorities
- Migrants and refugees
- Stateless populations or populations at risk of statelessness
- The elderly
- Persons with disabilities
- Non-nationals

As shown in Table 5, these characteristics have important implications for the design of new ID systems and the improvement of existing system.

Table 5. Design implications of status quo ID coverage

Coverage characteristic	Implications for Key Decisions
Low coverage for CR, ID, or similar foundational systems either overall or for specific groups	<p>Legal Framework: Identify any legal or procedural barriers to civil registration and ID and amend laws and procedures accordingly</p> <p>interoperability: Investments should be made to improve CR systems system in order to ensure identification from birth for the “flow” of newborns.</p> <p>Registration:</p> <ul style="list-style-type: none"> ▪ Extend eligible population to previously uncovered groups (e.g., children, non-nationals) ▪ Implement registration strategies that make enrollment easy and convenient and mitigate direct and indirect costs to registration, such as fees, travel time, transportation costs, lost wages, middlemen, etc. ▪ Implement targeted registration campaigns for excluded, under-covered, and other marginalized groups ▪ Identity proofing for the ID should not rely solely on possession of birth certificates or should include appropriate alternative methods (e.g., introducers) to ensure universal registration <p>Public Engagement:</p> <ul style="list-style-type: none"> ▪ Incorporate people-centric design approaches into the decision-making process for designing and implementing the ID system ▪ Continuous consultation with end-users and civil society to understand existing difficulties and desired improvements ▪ Implement strong information and awareness campaigns ▪ Adopt user-friendly grievance redress systems

3. Assess the trustworthiness of the system

As with coverage, the trustworthiness of existing ID systems—i.e., **whether or not they provide reliable sources of identity information and authentication, adequately protect personal data, and are trusted and used by people**—has implications for how these systems could be improved and/or leveraged by new ID projects. In this context, a number of characteristics are particularly important and should be evaluated by people familiar with the system:

- **Uniqueness**—the rate at which databases are free of duplicate identity records—i.e., the same person enrolled multiple times, under the same or different names—and credentials are unique to the individual (i.e., one person cannot have multiple of the same credentials, and/or multiple people cannot have the same credential). Uniqueness is important for some—but not all use cases.
- **Accuracy**—the rate of data entry errors, missing fields, or out-of-date attributes contained in identity records and/or credentials. Inaccurate data not only decreases the reliability and trustworthiness of the system for relying parties, it also has the potential to negatively affect people who are treated unjustly due to incorrect or out-of-date information.

- **Security**—the physical and cybersecurity of systems and data, and the resilience of databases, data transmissions, credentials, authentication mechanisms, and other systems to attempts at theft, hacking, fraud, spoofing, and cyber and other attacks, unauthorized access or disclosure, and misuse, as well as natural disasters, flooding, etc. Where security of the ID system is weak, this creates significant risks to privacy and data protection.
- **Confidence of the population**—whether or not people have confidence in the system and trust it with the collection and use of their data. The ability of people to have oversight and control over their data and how it is used, and their level of trust in the system overall are fundamental for the success of the system—if people do not trust or value identity systems, they are unlikely to use them.

Table 6. Design implications of the robustness of existing ID systems

Robustness characteristic	Implications for Key Decisions
Low uniqueness and accuracy of existing foundational ID registries	<p>Registration: If using existing data as a source for the new/improved system, it must be cleaned, deduplicated, and updated. This may require additional data collection and outreach efforts for data that the system does not already contain, or to replace low-quality data that is flagged or rejected during the migration. For example, biographic deduplication could help reduce the number of duplicates, depending on the quality of the data and other factors (e.g., the prevalence of dates of birth listed as “1 January”).</p> <p>Interoperability: Potential linkages between CR and ID to increase data accuracy</p>
Low uniqueness and accuracy of functional ID registries	<p>Interoperability: Data exchange or queries against a unique, accurate foundational system can potentially help clean up functional ID databases (e.g., removing duplicates and ghosts).</p>
Low security of existing identity databases, applications, and credentials	<p>Privacy and Security: Bring old or new systems into alignment with best-practice standards for data protection and privacy and adopt privacy and security measures throughout the lifecycle as the default setting.</p> <p>Registration: Consider the implications of insecure existing credentials for the identity proofing process in the new or upgraded system (i.e., will they provide a high enough level of assurance?)</p> <p>Credentials and Authentication: Adopt credentials with appropriate security features that protect personal data.</p>
Low confidence among the population	<p>Public Engagement: Practitioner’s should work to build trust in the new system through proactive and meaningful public consultations and communication campaigns.</p> <p>Privacy and Security: A data protection impact assessment may be required to address new privacy needs and to re-consider how legacy and new systems can better protect people’s data and build the confidence of the population.</p>

4. Evaluate the legal framework

A vital component of the existing ID landscape within a country are the laws and regulations that govern the ID system. In order to evaluate the legal framework, ID4D has created the *ID Enabling Environment Assessment (IDEEA)*, which is a supplementary tool to the *ID4D Diagnostic*. The IDEEA is a due diligence questionnaire that facilitates a systematic assessment of a country's laws, regulations, and institutions that enable and govern its ID systems, with the goal of identifying areas where administrative and legal frameworks might be strengthened to support the development of an ID system.

To begin, the assessment covers general laws, decrees, institutions and other frameworks that govern identity-related issues and data collection in general, including those dealing with:

- **Data protection and privacy**—existing laws and oversight institutions
- **Cybersecurity and cybercrime**—definitions of critical information infrastructure, oversight and regulatory institutions, criminalization of cybercrime, roles and mandates of central cybersecurity agency versus line agencies such as the ID authority.
- **International and extraterritorial issues**—data sovereignty, cross-border data transfers, and international functionality and recognition, and international conventions
- **Inclusion**—constitutional and legal provisions relating to minorities, discrimination, and citizenship
- **Other ID-related laws**—including limitations on a universal identifier, ID requirements related to passports and travel, exchange of health-related data, KYC requirements, SIM card requirements, e-Signatures, and more.

Next, it assesses the laws, regulations, and policies that enable and govern specific ID systems, including frameworks related to their:

- **Purpose and capabilities**—legal and regulatory definitions and capabilities
- **Institutional design**—administration, independence, roles, powers, interagency conflict, private sector involvement, financial sustainability, vendors technology and procurement
- **Inclusivity**—requirements regarding citizenship and legal status, age requirements, compulsory registration of births and deaths, the mandatory nature of IDs, fees, and barriers to inclusion
- **Lifecycle management**—registration, identifiers and credentials, use, storage and protection of personal data, and individual rights and protections

The completion of an *IDEEA* will help countries identify key areas of the legal framework that should be updated as part of a project to improve an existing ID system or create a new one. These findings will also impact key design decisions, as shown in Table 7.

Table 7. Design implications of existing legal framework

Legal system characteristic	Implications for Key Decisions
Insufficient, weakly enforced, or discriminatory laws and regulations related to ID	<p>Legal Framework: Adopt new—or amend existing—laws, decrees, institutions, and other frameworks to enable the ID system, empower ID providers and oversight agencies, remove barriers to inclusion, and protect privacy and personal data.</p> <p>Public Engagement: Conduct information campaigns and outreach to advertise changes in the law or procedure.</p>

Define Vision

An inclusive and trusted ID system can serve as a platform for broad administrative reforms and new modes of service delivery for both the public and private sector. As such, these systems may be implemented with a variety of purposes, including crosscutting goals and sector-specific use cases that become evident after the status quo analysis described above. **Defining a shared vision for ID and completing a full evaluation of potential current and future users will help ensure that system is fit for purpose and adaptable to long-term needs.** (See, for example, *Whitley & Hosein 2010*).

1. Define development goals

Depending on context, **ID projects may have different overarching goals that link closely with the country's economic and social development plans and cross multiple sectors.** The overall role or purposes envisioned for the ID system will have important implications for key decisions, and practitioners should design the ID system with these end goals in mind. Table 8. Design implications of potential cross-cutting goals for ID system

gives examples of some common cross-cutting goals and how these might factor into key design decisions for the ID system.

Table 8. Design implications of potential cross-cutting goals for ID system

Goal	Implications for Key Decisions
Increasing inclusion and meeting SDG 16.9 (“provide legal identity for all, including birth registration”)	<p>To improve inclusion and provide legal identity for all, ID systems should be designed to maximize coverage and minimize exclusion. This involves strengthening civil registration, identifying and removing or mitigating statutory, procedural, social, economic, and technological barriers to access through updates to the legal framework, choice of registration criteria and strategies (e.g., potentially de-linking identification from nationality, legal status, and other rights and entitlements), the choice of data to collect, adopting user-friendly and accessible credentials and authentication mechanisms, and engaging the public. Furthermore—in order to meet the goals of sustainable and inclusive development—measures should be taken to ensure that people who are unable to obtain identification are not excluded from the basic rights and services to which they are entitled.</p>

Goal	Implications for Key Decisions
Improving transparency and trust in government	When well-implemented, ID systems can serve as a foundation of trusted interactions between people and governments. This requires a legal and regulatory framework with sufficient safeguards, a privacy-and-security-by-design approach that gives people control and oversight over their data, and public confidence in the ID authorities themselves. The choices that practitioners make with regard to which data are collected, how the population enrolls in the system, the format of credentials (e.g., which data are visible), the adoption of privacy and security measures, and mechanisms for grievance redress are also likely to impact the degree to which people trust (or distrust) the system. Finally, the level of transparency and engagement with the public will be key to its successful adoption.
Digital transformation of services and economy	ID systems and other trust services like e-signatures can underpin the digital economy by providing on-demand, secure authentication of users, organizations, and devices to enable a variety of digital platforms and services (e.g., online tax filing, e-payments, commercial marketplaces). However, this requires credentials and authentication procedures that can be used in an online environment, with appropriate levels of assurance for different types of transactions. Furthermore, the use of open standards and platforms for interoperability can increase the utility of ID for third party platform developers. To understand and maximize the transformational potential of ID in the digital economy, practitioners should engage in in-depth consultation with the public and third parties to understand their needs, motivations, and acceptance of new ID services.
Reducing fraud and corruption	Strengthening identification and authentication can help prevent identity theft and identity-related fraud in both the public and private sector. In order to reduce identity-related fraud, ID systems must have high levels of assurance in identity proofing and authentication procedures. In some cases, this may include the collection of biometric data to de-duplicate identities and ensure uniqueness in the population. Linkages with the civil registry can also help prevent fraud by identifying deceased individuals. However, practitioners must evaluate the size of the fraud problem across various use cases, and carefully weigh these against other risks, such as preventing legitimate beneficiaries from accessing services to which they are entitled by virtue of overly stringent ID requirements. The levels of assurance adopted in various use cases should be proportional to the likelihood and impact of identity-related fraud.
Improve end-user experience with identification	In addition to improving trust, improvements to ID systems can also simplify users' experiences with identification and accessing public and private-sector services that require proof of identity. This requires designers to streamline the process and convenience of registering in the ID system and collecting and using credentials (e.g., the devices and hardware needed). Privacy-enhancing measures such as access portals that make it easy to control data use, as well as convenient grievance redress mechanisms can also improve the user experience.
Facilitating migration and trade	When mutually recognized by different countries, ID systems can simplify migration and cross-border economic activity. By adopting standards and trust frameworks for mutual recognition, designers can help ensure that ID systems are interoperable across borders to better facilitate movement and economic activity, including to act as a machine-readable travel document.

2. Define sector-specific use cases

In addition to overarching goals, identification can be a critical enabler for improving people's access to public and private services, and the efficiency and quality of these services. This includes potential applications of ID across the following sectors:

- Financial services
- Mobile and telecommunications
- Social protection
- Health care and insurance
- Education
- Agriculture
- Digital government
- E-commerce and digital trade
- Taxpayer identification and revenue generation
- Voter identification
- Property ownership and transfer
- Civil servant payroll management
- Passport issuance and border security

Depending on national priorities for the ID system, countries should consider how these various use cases may shape system design, as summarized in Table 9. Defining the desired use cases ahead of time is not only essential for building ID systems that are fit for purpose, but also for ensuring that the purposes for which the ID system will be used are well understood and accepted as well as pre-specified in the legal framework.

Table 9. Design implications of specific use cases

Use Case and Sectors	Implications for Key Decisions
Comply with identity-related requirements of know-your-customer (KYC) and similar regulations <ul style="list-style-type: none"> ▪ Financial services ▪ Mobile and telecom 	<p>In order to meet typical KYC requirements and customer due diligence (CDD) regulations related to identification and verification, identity proofing procedures should offer a high level of assurance. In addition, interoperability platforms that facilitate queries to verify an identity can also improve the efficiency of KYC verifications.</p>
Preventing identity theft and impersonation <ul style="list-style-type: none"> ▪ Financial services ▪ Mobile and telecom ▪ Digital government services ▪ Property ownership and transfers ▪ Taxation ▪ Sectors with cash/in-kind transfers ▪ Voter registration ▪ Border control 	<p>ID systems should offer a high level of assurance and adopt advanced security features and protocols to protect identities and personal data. Notification policies and easy-to-use grievance redress mechanisms should also be in place to deal with cases of stolen identities or data breaches.</p>

Use Case and Sectors	Implications for Key Decisions
Reducing fraud and leakage and improving targeting and service delivery for government programs <ul style="list-style-type: none"> ▪ Social protection ▪ Health ▪ Education ▪ Agriculture ▪ Civil service administration 	<p>In order to be useful for social protection programs—e.g., to identify beneficiaries—the target population (e.g., potential children, non-citizens) must be eligible for the ID well-covered. Leveraging the ID to prevent ghost, multiple, and/or fraudulent registration and improve targeting also requires some form of deduplication during the identity proofing process or in relying parties systems, and the ongoing removal of deceased persons through links with the CR system. Adopting standards and interoperability frameworks that allow for cross-checking and/or data exchange with other databases can also help prevent fraud, improve targeting, and ensure the portability of identities. In order to reduce instances of beneficiary impersonation, credentials and authentication mechanisms should offer a sufficient level of assurance.</p>
Facilitating new modes of service delivery <ul style="list-style-type: none"> ▪ Government service providers across all sectors ▪ Private companies that provide a variety of services ▪ E-commerce 	<p>Within the digital economy, innovations in service delivery will require secure digital credentials and authentication that can provide various levels of assurance for multi-modal authentication, as well as frameworks and services that allow various users to leverage these credentials for identity verification, authentication, and other trust services. As part of the innovation process, practitioners should also consult with end-users to understand existing difficulties and desired improvements</p>
Facilitating the use of anonymized data for the production of statistics <ul style="list-style-type: none"> ▪ Health ▪ Development planning ▪ Emergency response ▪ Academic researchers 	<p>In order to be useful for data collection, ID systems must have widespread coverage of the relevant population (e.g., CR systems must cover children if used as a source of infant mortality statistics). interoperability between systems such as ID, civil register, statistics, and sources of demographic and health data can also facilitate rapid detection and response to public health emergencies. However, data aggregation and sharing for public health, research, and planning purposes requires a robust legal framework and enforcement to protect privacy and personal data.</p>

Practitioners should adopt a risk-based approach to defining how ID will be deployed in various use cases. This approach should consider the level of assurance needed for various transactions to mitigate fraud and other risks, as well as the potential for exclusion and privacy violations involved with requiring identification or authentication for different purposes. For example, requiring people to have an ID for services that previously did not require one may prevent people who face significant barriers to obtaining an ID—e.g., vulnerable and marginalized groups, low income people, women, etc.—from being able to access crucial support. See [CIS \(2019\)](#) for one approach to considering when ID should (and should not be) applied.

Identify Constraints

The choices that a country makes for its ID system are shaped by multiple constraints. Understanding and addressing these constraints through system design is vital for ensuring that the ID system is

successful and fit-for-purpose. Adopting technologies that are impractical for the country context or unusable by a large share of the population will seriously limit the potential benefits of identification.

1. Assess the country's digital infrastructure

Many aspects of a modern ID systems rely on digital infrastructure, including **internet connectivity**, **mobile phone coverage**, **smart phone ownership** and **electrification**. Weak connectivity and digital infrastructure therefore have important implications for design choices:

- Without reliable internet connections at registration centers, data must be stored locally and then physically transferred to a location with connectivity for uploading to the ID system. This can create risks to data security and loss (and inaccuracy if data is collected on paper first and subsequently entered into a database) and lengthens the timeline for identity proofing.
- The capture of digital data—such as biometrics—also requires power, either through permanent electrification or solar or battery-powered kits.
- Many forms of digital authentication, as well as ID-related services such as personal access portals, require internet or mobile phone connectivity, to which many people may not have access, and a connection to a reliable national backbone, which may not exist in all countries. Other solutions require the distribution of hardware (e.g., card readers) that may also require electrification.
- ID systems require secure data centers with a constant electricity as well as back-ups and disaster recovery solutions in the case of power outages, riots, or natural disasters.

Practitioners should assess the country's overall digital infrastructure and consider the implications for key decisions presented in Table 10.

Table 10. Design implications of digital infrastructure

Digital infrastructure characteristic	Implications for Key Decisions
Low internet connectivity across the country	<p>Registration:</p> <ul style="list-style-type: none"> ▪ Registration strategy and cost, including the choice of registration points and technology ▪ Identity proofing requirements and processes ▪ Ensure that if internet crashes, data is temporarily saved locally (and encrypted) on enrollment kits for asynchronous uploading <p>Credentials and Authentication:</p> <ul style="list-style-type: none"> ▪ For credentials that are not issued on the spot, will need to devise offline methods of ensuring that the credential is bound to the person who enrolled ▪ Online authentication may not be feasible in remote areas, requiring alternate authentication mechanisms <p>IT Systems:</p>

Digital infrastructure characteristic	Implications for Key Decisions
	<ul style="list-style-type: none"> Cloud-based storage may not be an option, depending on the requirements for availability
Low electrification across the country and/or frequent blackouts	<p>Registration:</p> <ul style="list-style-type: none"> Registration strategy and cost, including the choice of registration centers and technology (e.g., battery or solar-powered kits) Identity proofing requirements and process will need to operate in low-power environments <p>Credentials and Authentication:</p> <ul style="list-style-type: none"> Some digital authentication may not be feasible in remote areas, requiring alternate authentication mechanisms <p>IT Systems:</p> <ul style="list-style-type: none"> Data centers and disaster recovery sites require backup power sources; cloud-based technologies may be an option
Low internet/mobile coverage among segments of the population	<p>Credentials and authentication:</p> <ul style="list-style-type: none"> Types of credentials issued should be accessible to all Mobile-based credentials and authentication should not be the only way to prove one's identity <p>Public engagement:</p> <ul style="list-style-type: none"> Certain platforms and services may not be universally accessible

2. Evaluate needs based on geography and population size

A country's geography and population—including total **size**, **population density**, **terrain**, **road conditions**, and **high-risk areas**—can have important implications for the strategies and technologies required for registration as well as the overall cost of implementing an ID system. For example:

- The logistics and timeline of an initial registration campaign increase with the size of the territory as well as the frequency of sparsely populated areas, with implications for cost.
- The size and demographics of the population has implications for overall system cost and technology choices (e.g., if a country is using biometrics, multimodal biometrics are needed to strengthen the accuracy and efficiency of deduplication for large populations).
- Difficult terrain—e.g., dense forests or jungles, mountains, islands, rivers, deserts, etc.—and poor road conditions may necessitate supplementary modalities and technology for registration, such as mobile units in trucks, boats, motorbikes, helicopters, etc.
- Areas with security concerns may need additional strategies for registration, as well as measures such as enhanced security of personnel and assets.

Given the potential difficulties associated with certain geographies, as well as difficult roads and transportation, there is a high risk of exclusion for remote or difficult to reach populations. To mitigate these risks, practitioners should consider the implications of certain geographic constraints on the design and rollout of their ID system, including those outlined in Table 11.

Table 11. Design implications of geography

Geographic characteristic	Implications for Key Decisions
Large territory and/or many sparsely populated areas	Registration: <ul style="list-style-type: none"> Registration strategy, timeline, and cost, including measures to reduce the direct and indirect costs of people having to travel long distances, and bring enrollment services close to the people
Population size and growth rates	Registration: <ul style="list-style-type: none"> Registration procedures and timelines should reflect population size Consider sufficient enrollment infrastructure for densely populated areas to avoid long wait times Data: <ul style="list-style-type: none"> Sufficient data points are needed to deduplicate the population (e.g., multiple biometrics if using biometric recognition) Data storage and systems capacity must be appropriate to handle the current and projected population
Difficult terrain and/or areas with security risks	Registration: <ul style="list-style-type: none"> Registration strategy, timeline, and cost, including the choice of enrollment centers and technology (e.g., mobile units) Public engagement: <ul style="list-style-type: none"> Information campaigns and outreach must be tailored to and accessible to remote populations Special efforts should be made in high-risk areas to ensure sufficient outreach and trust with the population

3. Consider socioeconomic characteristics

Ideally, an ID system will help contribute to inclusive economic, social, and political development. However, current levels of social and economic development and overall population characteristics—including **poverty rates**, **general and technological literacy levels**, and the prevalence of **persons with disabilities**—also have important implications for the architecture of ID systems. If these factors are not incorporated into design, the ID system may not be easily accessible to large groups of marginalized people, increasing the risk of exclusion. In particular:

- The direct and indirect costs of registration and obtaining credentials will disproportionately affect poor and rural people; who may make up a large portion of the population and are also those for whom identification may have the highest marginal benefits.

- People who cannot read may have trouble completing registration forms and remembering or using ID numbers and PINs.
- Persons with disabilities may constitute a large portion of the population and will require specific accommodations for registration and utilization of the ID system; if biometrics are being used, persons with disabilities as well as elderly persons and manual laborers and other groups, may have difficulty giving fingerprints.
- Digital illiteracy and poverty may also make it difficult for some people to access or use certain features of ID systems, such as mobile or internet-based applications.

Table 12 presents some important implications of socioeconomic development for design. In particular, registration and outreach strategies should be designed to foster inclusion of marginalized groups.

Table 12. Design implications of socioeconomic development

Socioeconomic characteristic	Implications for Key Decisions
High poverty rates	<p>Administration:</p> <ul style="list-style-type: none"> ▪ Fee charging models must not price people out of the ID system either through access to the ID system or related services <p>Credentials and authentication:</p> <ul style="list-style-type: none"> ▪ First credentials should be free of cost to the individual <p>Registration:</p> <ul style="list-style-type: none"> ▪ Registration strategy should attempt to mitigate direct and indirect costs of enrollment and collecting credentials
High rates of elderly persons, general illiteracy, technological illiteracy, and/or disability	<p>Registration:</p> <ul style="list-style-type: none"> ▪ Staff should be trained to assist the elderly, people with low levels of literacy, and people with disabilities to complete applications and other requirements <p>Credentials and authentication:</p> <ul style="list-style-type: none"> ▪ The types of credentials and authentication mechanisms should be accessible to the elderly, people with lower levels of literacy, and people with disabilities <p>Privacy and Security:</p> <ul style="list-style-type: none"> ▪ Platforms for personal oversight over data (e.g., personal records) may not be universally accessible <p>Public engagement:</p> <ul style="list-style-type: none"> ▪ Information campaigns should involve methods of communication (e.g., radio, television) that are accessible to illiterate people and those with disabilities ▪ Civil society and other organizations should be engaged to assist people with registration

In addition to these socioeconomic characteristics, the general **wage levels** within the country will also have important implications for the cost of the ID system associated with labor and human resources.

4. Consider cultural and historical relationship with ID

There may be certain **social norms, cultural and religious practices**, and **historical factors** that need to be considered when designing an ID system. These vary dramatically by country, but could include:

- A linguistically diverse population who will need outreach in various languages
- Traditional practices regarding the naming of newborns that affect timely birth registration
- Certain groups who are opposed to identification for cultural or religious reasons or because of past discrimination
- Social norms that limit the mobility of certain groups, such as girls, women and persons with disabilities

Addressing these issues—as indicated in Table 13—is crucial for ensuring the inclusion of potentially marginalized groups and building trust in the ID system.

Table 13. Design implications of cultural and historic factors

Cultural characteristic	Implications for Key Decisions
Linguistically diverse population	<p>Registration:</p> <ul style="list-style-type: none"> ▪ Registration agents should include staff who speak local languages and/or sign languages ▪ Registration forms should be translated into local languages <p>Public engagement:</p> <ul style="list-style-type: none"> ▪ Information campaigns should include multiple languages and through multiple channels (e.g., radio, television, and print) ▪ CSOs and other organizations should be engaged to assist minority language speakers
Identification is a cultural or religious taboo or historically sensitive (for certain groups or the entire population)	<p>Administration:</p> <ul style="list-style-type: none"> ▪ ID provider should be a neutral entity that instills trust in the system <p>Data:</p> <ul style="list-style-type: none"> ▪ Data collected should be minimal and not include sensitive information that may be perceived as a tool for discrimination (e.g., religion) or violates cultural norms (e.g., biometrics) <p>Registration:</p> <ul style="list-style-type: none"> ▪ Registration procedures and data collection should be done in a culturally and religiously appropriate manner (e.g., female-only enrollment teams may be required in some communities) <p>Public engagement:</p>

Cultural characteristic	Implications for Key Decisions
	<ul style="list-style-type: none"> Information campaigns and public consultation should involve outreach to skeptical or marginalized groups CSOs and other organizations should be engaged to facilitate participation
Low mobility for certain groups (e.g., girls, women, persons with disabilities)	<p>Registration:</p> <ul style="list-style-type: none"> Registration strategy (e.g., mobile and/or female-only units) that bring ID services closer to the people and conform with social norms <p>Public engagement:</p> <ul style="list-style-type: none"> Information campaigns should involve outreach to low-mobility groups and religious and community leaders as appropriate CSOs and other organizations should be engaged to assist low-mobility people and persons with disabilities with registration

5. Assess timeline requirements

Implementing an ID system with full coverage generally takes time, from multiple years to a decade. However, there may be pressing needs for the ID system, such as an election or the rollout of a cash transfer linked to subsidy reform. Although rushing the rollout of the ID system will likely reduce the inclusivity and trustworthiness of the system and is not advised, there may be certain design choices that can provide staggered functionality without compromising quality and longer-term coverage.

Table 14. Design implications of timeline constraints

Timeline characteristic	Implications for Key Decisions
Short to medium-term use-case for specific populations (e.g., elections, social transfer)	<p>Registration:</p> <ul style="list-style-type: none"> Registration strategy could involve a staggered approach, targeting relevant populations first (e.g., voters over age 18, or low-income residents for a cash transfer), and also include mobile units and mass-campaigns <p>Public engagement:</p> <ul style="list-style-type: none"> Intensive information campaigns and outreach to facilitate high coverage in a short amount of time CSOs and other organizations should be engaged to people to speed up registration and reduce the potential for exclusion

Evaluate Costs and Benefits

Well-designed ID systems have the potential to advance multiple development goals and create fiscal savings for governments by increasing administrative efficiency, reducing fraud, and improving taxation. However, they also require a significant investment. The specific cost drivers in a given context are a function of inherent country characteristics as well as the overall system design. Understanding the cost implications—and potential fiscal benefits—of different components of the

ID system will help practitioners make smart investments in vital areas while avoiding expensive solutions that may not serve the country's ultimate goals or needs.

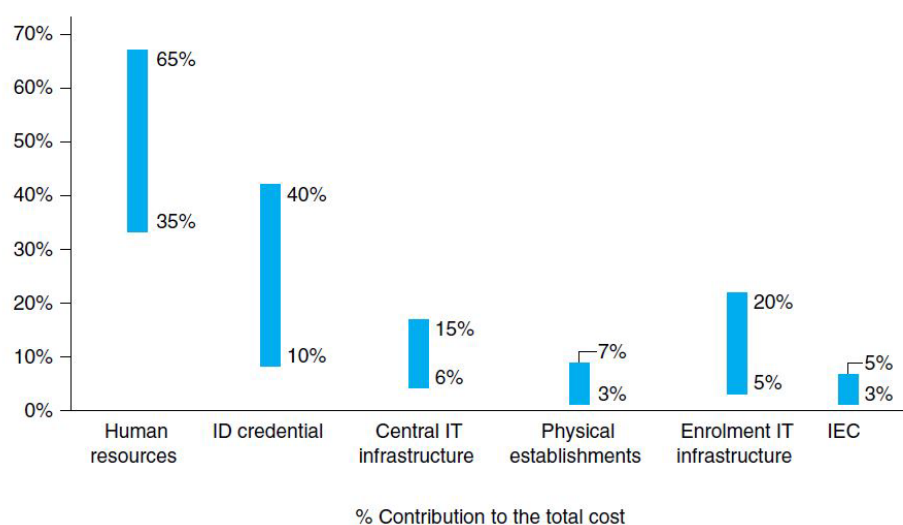
As part of the planning process, practitioners should make a complete cost-benefit analysis (CBA) of different technical and implementation options. This includes modeling costs for ID system features and roll-out strategies, as well as identifying potential fiscal and non-fiscal benefits to the government, private sector and individuals. ID4D has developed several tools to assist with this process, including:

- A toolkit that explains *cost drivers* and a *costing model (Excel)*
- A framework for estimating potential *fiscal saving for the public sector*
- A framework for estimating potential savings for the *private sector and broader economy*

1. Estimate cost implications of ID systems

Using data from 15 countries at various levels of development and with diverse ID ecosystems, the ID4D costing study identified **six key categories that together make up 90 percent of the typical cost of ID systems**: (1) human resources, (2) credentials, (3) central IT infrastructure, (4) physical establishments, (5) registration infrastructure, and (6) information and education campaigns (IECs) (see Figure 8).

Figure 8. Major cost categories for ID systems



Source: *Understanding Cost Drivers of Identification Systems*

As shown in Figure 9, the **major drivers that determine expenses within these categories** include country characteristics and design choices. For system design, the highest impact drivers are related to many of the key decisions discussed above, including:

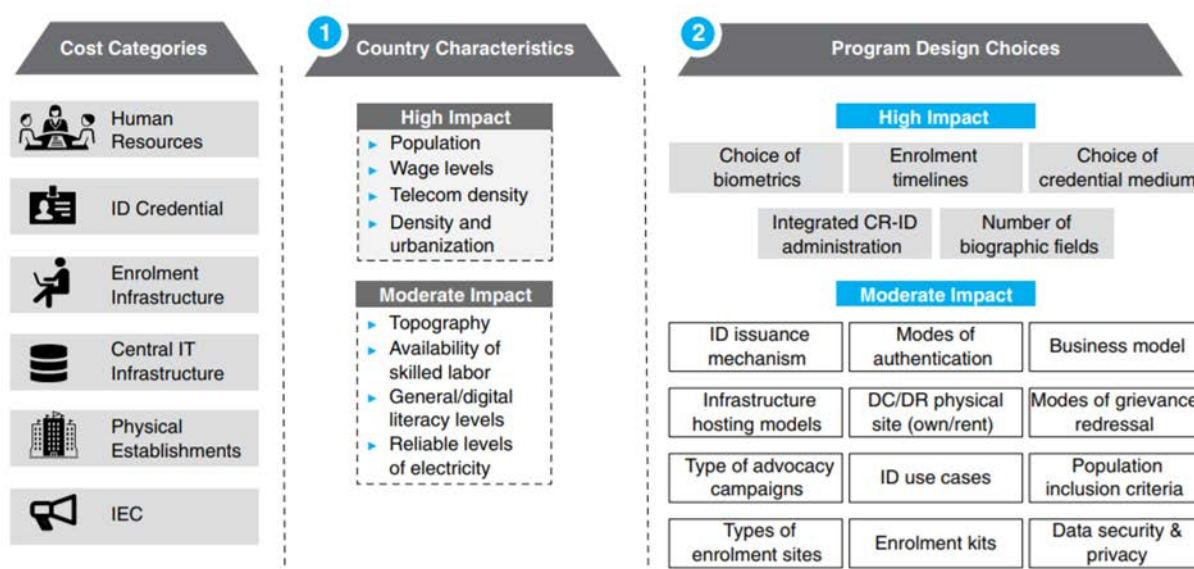
- **Registration timeline:** Countries with shorter timeframes (~2 years) experienced higher costs due to the personnel and equipment required to enroll large portions of the population

simultaneously in a short amount of time. Countries with a longer time frame (~3-6 years) had a lower and more uniform distribution of costs.

- **Choice of biometrics:** Each additional multimodal biometric modality captured (i.e., fingerprints, facial image, iris scans) increased cost by approximately 5-10 percent; however multimodal biometrics also increase accuracy and inclusion compared with single modality approaches.
- **Number of biographic fields:** The number of data fields captured determines the time to collect, digitize, and proof identities, and its associated human resource costs. Furthermore, the more semi-static data collected during (e.g., address, email), the more time and resources will be spent in the future on updating this data.
- **Choice of credential form factor:** Physical credentials (i.e., cards) have the highest variation in cost, with estimated expenses between 10 to 40 percent of the total project costs. The low end of the cost spectrum includes very basic ID cards with the capacity for online authentication, while the higher costs are associated with multi-purpose smartcards.
- **Integration between CR and ID:** Countries where CR and ID systems were closely integrated—e.g., through a unique ID number (UIN) issued at birth and shared administration—had substantial savings in both the start-up and steady-state phases of the project.

In addition to these design choices, the study also identified procurement practices as a major potential cost inflator.

Figure 9. Cost categories and drivers for ID systems



Source: *Understanding Cost Drivers of Identification Systems*

In addition to design choices, many of the same country characteristics that influence design decisions will also influence costs. The highest-impact characteristics include:

- **Population size:** Countries with a larger eligible population often require a greater investment to adequately meet the enrollment targets and timelines for the ID program. At the same time, a larger population could also result in reduction of program cost per person (e.g. central infrastructure costs) due to economies of scale.
- **Density and urbanization:** High urbanization levels and population density have a considerable impact on the distribution of human resources, registration centers and kits for the program. Countries will have to deploy more program resources towards urban centers than to rural centers, but the marginal cost of reaching an additional person is typically lower than in remote areas.
- **Labor and wage levels:** Human resources (e.g. program staff for central administration, enrollment and resident engagement) are one of the major drivers of ID system cost. Therefore, the prevalent wage levels in the country will have a significant impact on the operating cost, across both during the start-up phase and steady state of the ID program.
- **Digital infrastructure:** Existing ICT infrastructure influences design choices (e.g., credential types and online authentication mechanisms) that drive the cost of the overall program. In addition, lack of infrastructure at registration stations that limits the ability to securely enter and transfer data will lengthen the timeline, also potentially inflating costs. The need to connect remote centers (e.g., via wired or wireless connections) will significantly increase cost. Finally, the extent to which capacity building is required (e.g., for cybersecurity protections) also needs to be considered.

Practitioners can use the *costing model spreadsheet (Excel)* developed through the *ID4D Costing Study* to estimate the costs of their own ID systems by manipulating different country characteristics and design choices.

2. Determine opportunities for savings

In addition to the cost of specific design choices, practitioners should also consider their potential fiscal benefits. A pair of ID4D publications create a framework for estimating these potential benefits across sectors (see *ID4D Public and Private Sector Savings*). In particular, these papers highlight important features of ID systems that enable these savings, including (1) digitization, (2) a unique ID, (3) integration and interoperability, and (4) digital authentication, as shown in Table 15. For the private sector, additional features are (5) queriability, and (6) public-private partnerships (PPPs).

Table 15. ID system features that generate savings in the public sector

Feature	Description	Key Benefits
Digitization	Transition from paper to digital-based systems, including of databases, credentials, data transfer, etc.	<ul style="list-style-type: none"> ▪ <i>Direct:</i> reduces operating and transaction costs ▪ <i>Indirect:</i> enables deduplication, integration/interoperability, and digital authentication
Uniqueness	Creation of a unique identifier—potentially though not necessarily via biometrics—for each person enrolled in a specific ID system.	<ul style="list-style-type: none"> ▪ <i>Direct:</i> prevents some types of fraud ▪ <i>Indirect:</i> enables integration/interoperability
Integration & Interoperability	Coordination and connections between different ID systems, including the ability to exchange information.	<ul style="list-style-type: none"> ▪ <i>Direct:</i> reduces operation and transaction costs; enables identity verification and authentication services across systems
Digital Authentication	Electronic process that uses one or more factors to confirm that someone is who they claim to be	<ul style="list-style-type: none"> ▪ <i>Direct:</i> decreases risk of impersonation; reduces transaction costs; enables fee-based models for authentication services

Source: Adapted from *Public Sector Savings and Revenue from Identification Systems*

ID systems that include these features may enable a number savings and revenue-generating mechanisms, as shown in Figure 10. A thorough assessment of potential mechanisms should be conducted in the planning stage of an ID system to fully estimate the economic impact of these investments. See the *public sector savings paper* for a walk-through of this assessment and for country examples.

Figure 10. Savings and revenue-generation mechanisms

	A. Decreasing Expenditures	B. Increasing Revenue	C. Economic Climate
Public Sector	<ul style="list-style-type: none"> ▪ Reducing fraud in G2P transfers—by removing ghosts, duplicates, and ineligible beneficiaries, and reducing impersonation ▪ Reducing administrative costs by eliminating redundant systems and reducing transaction costs 	<ul style="list-style-type: none"> ▪ Increasing tax collection by widening the tax base and identifying cases of fraud ▪ Charging fees for select identity services such as authentication and verification of identities for relying parties 	
Private Sector	<ul style="list-style-type: none"> ▪ Reducing theft and fraud through better identification of clients ▪ Reducing operational costs associated with compliance, liability, administration, and transactions 	<ul style="list-style-type: none"> ▪ Increasing customer base for services that require trusted identification ▪ Decreasing customer abandonment and rejection due to easier, more accurate identification ▪ Charging fees for identity-related services (e.g., as a PPP) or add-ons 	<ul style="list-style-type: none"> ▪ Creating a “business friendly” environment overall due to improved trust in identity-related services and improved administrative efficiency

Source: Adapted from *Public and Private Sector Savings reports*

Assess Risks

1. Evaluate risks to privacy and data protection

Any activity that collects, stores, processes, generates, and/or utilizes personal data must contend with the risk that this data might be stolen, misused, or mismanaged, with negative consequences for the individual. Evaluating and mitigating risks to digital privacy and data protection (see Box 5 for definitions) is therefore essential for the success of an ID system.

Box 5. Defining privacy and data protection in the ID system context

The concept of **digital privacy** can be understood as the *appropriate and permissioned use and governance of data*. This differs from the fundamental right to privacy, commonly understood as the “right to be let alone.” In ID systems, data privacy does *not* necessarily mean that all data is kept secret at all times. Rather, it means that data should only be accessed, processed, or shared by and with authorized users for pre-specified purposes that have been agreed in advance.

Data protection—which includes the legal, operational, and technical methods and controls for securing information and enforcing rules over access and use—is therefore fundamental to ensuring data privacy.

Personal data, also referred to more narrowly as personally identifiable information (PII) refers to “any information relating to an identified or identifiable natural person”—also known as a **data subject**—which is a person “who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (GDPR, Article 4).

Personal data is sometimes divided into a subset known as **sensitive personal data**, which is personal data that, by their nature, merit specific protection as the context of their processing could create significant risks to a person’s fundamental rights and freedoms. They include data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, health, life or sexual orientation, as well as biometric and genetic data (e.g., see GDPR Recital 51).

The responsibilities of those using personal data are complemented by the rights of data subjects—e.g., people who have registered in an ID system—such as the **right to have control over one’s own personal data**, including the corrections or modifications.

Any activity that collects, stores, or processes personal data raises certain risks, including, but not limited to:

- **Security breaches:** Physical or cyberattacks on databases or during data transfer.
- **Exposure of sensitive personal information:** Disclosing sensitive personal information (e.g., biometrics, religion, ethnicity, gender, medical histories, etc.) for unauthorized purposes.
- **Unauthorized disclosure:** Inappropriate transfer of data between government agencies, foreign governments, private companies, or other third parties.
- **Function creep:** Using and disclosing personal data that was collected for one purpose for other purposes without a person’s consent.

- **Surveillance:** Tracking people as they go about their daily activities by the public or private sector (e.g., using artificial intelligence and advanced data analytics).
- **Discrimination or persecution:** Data collected and/or stored on credentials is used to profile individuals and discriminate against or persecute them based on their identity.
- **Unjust treatment:** If the data collected are incomplete or inaccurate, this can lead to mistaken identity or unjust treatment.
- **Identity theft and fraud:** With access to people's personal data (and particularly in combination with unique identifiers), criminals may steal or synthesize people's identity information and then impersonate them for financial or other gain (e.g., opening bank accounts or applying for credit in their name, falsely claiming government benefits, using the stolen identity to commit crimes or evade background checks).

Although these risks are present in any ID system, **digital ID systems can amplify them and increase the scale of their consequences.** For example, digital ID systems present considerable cybersecurity risks in the form of penetration by hackers, hacktivists, cyber-criminals or cyber-terrorists to access or steal identity data or to compromise the integrity or functionality of the system. Their purposes can range from making financial profit to making political demands. These threats need not emanate only from cyberspace—human and physical vulnerabilities can play a key role in allowing attackers access to sensitive systems.

Table 16. Threats to privacy and data protection throughout the identity lifecycle

Data Processing Activity	Potential Threats and Vulnerabilities
Collecting data	<ul style="list-style-type: none"> ▪ No consent given ▪ Forced consent/no choice ▪ Illegal/unfair/excessive collection ▪ Unsecured collection ▪ Misleading or unspecified purpose for collection ▪ Unauthorized/uninformed secondary purpose for data ▪ Tracking or surveillance using the metadata of transactions related to the identity
Storing, transmitting and using data	<ul style="list-style-type: none"> ▪ Illegal access/usage ▪ Sale of data ▪ Negligent usage/misuse ▪ Invasion of privacy ▪ Error in processing (e.g., disclosing data in error) ▪ Inaccurate/outdated data (e.g., regarding consent) ▪ Database hacked ▪ Phishing ▪ Monitoring transactions
Retention of data (long-term storage)	<ul style="list-style-type: none"> ▪ Loss of Data ▪ Unlimited Retention ▪ Unsecured data ▪ Virus/malware/ransomware ▪ Data compromised ▪ Lost device

Data Processing Activity	Potential Threats and Vulnerabilities
	<ul style="list-style-type: none"> ▪ Unprotected device ▪ Lost archives ▪ Identity theft ▪ Technology obsolescence
Data disposal and data sharing	<ul style="list-style-type: none"> ▪ Improper Disposal ▪ Unauthorized disclosure to third parties ▪ Forced opt-in for unspecified data sharing ▪ Social engineering ▪ Misrepresentation ▪ Confidentiality breach ▪ Illegal access ▪ Denial of access ▪ Insecure Transmission

Source: Adapted from a presentation of the Philippines Data Protection Agency and Shepherdson et al. 2016.

In addition, digital ID systems also amplify certain risks due to the ease and speed with which digital data can be transferred, copied, or destroyed, the ability to collect and correlate large amounts of data, and advanced analytics. In addition, particular design choices augment certain risks to digital privacy, including collecting large amounts of data, storing data in centralized databases, using a unique identifier across multiple systems, sharing data across agencies or systems, and collecting certain types of data (e.g., sensitive biographic information and biometrics). Conversely, digital technologies also have advantages regarding privacy and the security of data (e.g. easier to correct data, stronger access control, and enhanced auditability, including through immutable record-keeping) when compared to analogue/paper methods of collecting and managing data.

In order to mitigate the above risks, practitioners should implement multiple, adequate solutions to ensure that these systems merit people’s trust and protect personal data to the highest standards, including:

- **Adopting a comprehensive legal and regulatory framework for the processing of personal data:** This includes strong data protection and privacy laws, institutional oversight, and clear lines of authority and accountability that meet existing and emerging standards in national, regional, and international law. There should also be clear and accessible mechanisms for reporting of misuse and/or fraud and obtaining redress should a person’s identity be compromised.
- **Implementing other operational and technical controls that follow a “security-and-privacy-by-design” approach:** Privacy and security controls that meet global standards should be built into ID system technology and processes in order to comply with the legal framework and protect against the threat of security breaches, unauthorized disclosure, function creep, surveillance, while giving people more control over their data.
- **Ensuring that ID systems do not serve as a tool for discrimination or persecution:** Certain groups—such as ethnic, racial, or religious minorities—may face particular privacy concerns regarding the collection and use of data that indicates their group identity, and which could

be used to profile or discriminate against them. Practitioners should carefully consider risks to these groups from collecting sensitive information—including biometrics—and adopt sufficient legal and procedural protections against discrimination.

- **Pro-active consultation and communication:** In some cases, mistrust in the system could be the result of a lack of information. In order to pre-empt and/or mitigate these concerns, practitioners should implement outreach and education campaigns early-on to consult with the public on privacy and data protection issues and ensure effective and transparent communication about the purpose and use of these systems and the protections they offer.
- **Identifying risks to be mitigated through a data protection impact assessment (DPIA):** Conducting a DPIA is recommended to evaluate the impact of the ID system on personal privacy and data and articulate how various controls will help mitigate these risks.
- **Undertaking threat modeling exercises:** Before procurement, practitioners should undertake a threat modeling exercise to assess potential internal and external threats throughout the identity lifecycle (see Table 16 for examples of potential vulnerability at different stages of data processing). This is crucial not only for the security of the system, but to ensure uptake—people are less likely to participate in an ID system if they fear that their data will be misused or mismanaged.

In addition, practitioners should conduct regular audits of the legal, technical, and procedural security measures to ensure that personal data is well protected. **Importantly, however, it is not possible to guarantee the complete safety of a system from an attack.** Hackers who are intent on penetrating the system and are equipped with the appropriate resources spanning financing, talent and time will eventually succeed—e.g., as they did in the 2015 breach of the U.S. Office of Personnel Management that targeted the records of 21.5 million people or the 2017 Equifax breach that affected over 148 million people (see <https://www.opm.gov/cybersecurity/cybersecurity-incidents/> and <https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement>). The key to protection is to detect threats early and respond quickly—**only by taking data protection seriously will digital ID systems live up to their transformative potential.**

2. Evaluate exclusion risks

Well implemented ID systems have the potential to facilitate inclusive development by providing people with a trusted way to prove who they are and thus removing a potential barrier to the access of rights and services. In addition, they can allow service providers to utilize digital technology to expand or innovate how those services are offered. At the same time, there is the risk that these systems may also lead to the exclusion of certain individuals or groups through:

- **Statutory exclusion from the ID system:** Some ID systems are designed to cover only a portion of the population, such as national IDs that are issued to citizens over the age of 16 or 18. In such cases, groups that do not meet the inclusion criteria (e.g., due to age, nationality) are excluded from an ID system by design. If these individuals do not have access to other government-recognized ID systems (e.g., if birth registration for children is low or if refugees cannot access identification recognized by the host State), they may be unable to prove their legal identity—which is the subject of SDG target 16.9—or access services.

- **Unintentional exclusion from the ID system:** Frequently, there are groups—such as the poor, rural populations, the elderly, marginalized women and girls, persons with disabilities, stateless persons, refugees, etc.—that face significant economic and social barriers to enrolling in or using the ID system. Unless the ID system and its implementation are designed to help people overcome these barriers, it is likely that large and already vulnerable segments of the population will have lower rates of coverage.
- **Exclusion from associated rights and services:** The above groups of people who were unable to register or who are unable to easily use the ID system will then face barriers to accessing the rights and services for which this ID is required. This is a particular concern when ID is formalized and mandated in a context where a large portion of the population previously lacked government-recognized identification but may have been able to access services through informal or alternate methods of identification. In such cases, people who could previously get by without formal identification may now find themselves unable to complete basic transactions that require the new ID. For example, a potentially stateless population (e.g. ex-refugees) may have lived and been accepted in a community for years or even generations and received some kind of social benefits (e.g. cash transfers), but their access to these entitlements may be made more difficult if they are unable to register for a new ID due to the lack of conclusive evidence of their nationality, and this ID becomes mandatory for access to services.

In order to mitigate these risks, practitioners should undertake a thorough assessment of groups that may be vulnerable to exclusion and the barriers they may face when attempting to enroll in or use the ID system and access related rights and services. Important groups that may experience difficulties with identification typically include:

- Minors, including orphans and other vulnerable children
- Women and girls
- Minority groups (e.g., ethnic, linguistic, religious, political, etc.)
- Migratory groups (e.g., pastoralists and nomadic peoples, etc.)
- Non-nationals, including migrants, refugees, and asylum seekers
- Stateless persons
- Nationals who lack proof of nationality
- Internally-displaced persons
- Gender and sexual identity minorities
- Poor people
- Rural dwellers and other geographically isolated communities
- The elderly
- Persons with disabilities
- Illiterate people

As shown in Table 17, these groups may face a variety of barriers to enrolling in or using ID systems, including:

- **Legal or statutory:** Certain laws, including those that define who is included in the ID system, regulations, and policy frameworks that relate to citizenship, statelessness, and birth registration may prohibit certain individuals from participating in an ID system, or may create disincentives for registration. For example, laws that require marriage certificates for birth

registration may prevent unmarried women or those with customary marriages from registering their children. In addition, penalties for late birth registration may disincentivize parents from registering their children. Similarly, national ID laws that restrict these systems to only nationals exclude non-nationals and/or those who cannot prove their nationality. In addition, the strict requirement of a birth certificate for enrollment is likely to create a barrier for many adults who may not have had their birth registered decades earlier, but still hold other reliable forms of identification (e.g., a passport or driving license).

- **Procedural:** The policies and processes that govern how individuals enroll in and use ID systems may also create barriers to participation, including complex logistical requirements—e.g., requiring supplementary documentation that necessitates multiple visits to government offices—and the location, hours, and the staffing of registration centers. For people who speak minority languages or persons with disabilities, enrollment in ID systems may also be hampered when registration procedures and staff do not adequately take their needs into account.
- **Economic:** Charging fees for registration or obtaining a credential may be cost-prohibitive for poor people. In addition, complex procedural barriers may also create indirect costs, such as travel expenses, lost wages, and fees paid to agents or intermediaries. If fees are charged for identity authentication and verification, and such fees are passed on to people by service providers, this can also create costs for accessing services that create a barrier for poor people.
- **Social, cultural, and religious:** Multiple groups may face social barriers to participating in ID systems. In some contexts, for example, women and girls have less mobility and may not be able to reliably visit registration centers. Enrollment requirements that force people to remove specific garments (e.g., headscarves for women) or break religious practices may create additional barriers. In addition, certain groups, including ethnic and religious minorities may be reticent to participate in ID systems if they fear persecution or misuse of their data.
- **Technological:** Certain types of digital ID systems, including online authentication and mobile ID applications that rely on smartphones may not be accessible to poor people, those in lower connectivity areas, as well as people who are digitally illiterate. In addition, certain modalities of biometric recognition may present difficulties for certain populations (e.g., children, the elderly, persons with disabilities, manual laborers, etc.).

Identifying vulnerable groups and the barriers they face should involve multi-stakeholder consultation, including input and information gathering sessions with the public and civil society organizations that advocate for vulnerable groups. The **IDEEA** also provides additional tools for evaluating statutory and procedural barriers to registration.

Table 17. Common vulnerable groups and barriers to registration and use of ID

Group	Statutory	Procedural	Economic & Social	Technological
Children	May not be included in the ID system; some regulations for birth registration (e.g., requiring marriage certificates or national IDs of parents) may deter registration	The absence of a parent or legal guardian can pose challenges for registration because of the requirement for their consent prior to data collection		Difficulty capturing biometrics in young children; risk that biometrics captured from a young age will become out of date if not regularly updated
Women and girls	Some countries have different requirements for men and women to enroll for ID	Women may face harassment when they attempt to enroll in or use the ID system; some centers may have insufficient female staff or no female-only facilities in contexts where this is socially required (see economic and social barriers)	Women and girls may have less mobility in (e.g., difficulty leaving the house without a male relative), some procedures may run counter to religious practice (e.g., removing face coverings or physical contact with non-male relatives)	
Ethnic, racial, or religious minorities	Some laws and regulations (e.g., around nationality) may discriminate based on ethnicity, race, or religion	Individuals may face discrimination when they attempt to enroll in or use the ID system	Groups with a historical mistrust of government that fear profiling or persecution may be reluctant to participate in an ID system or to engage with any government service.	
Linguistic minorities		Enrolling in and using the ID may be difficult if staff do not speak local languages and/or application forms have not been translated		Credentials may be difficult to use if they are not in local languages; translated or transliterated names and other information may be inaccurate
Migrants	May not be included in the ID system	May face challenges accessing proof of immigration or visa status, if this is a requirement for registration in an ID system	Even if included in the ID system, persons with an irregular migration status may be reluctant to apply for fear of immigration enforcement or other negative consequences	
Nationals without proof of nationality		May be unable to enroll with extensive and inflexible identity proofing requirements for nationality (e.g., a birth certificate) or unclear or weak administrative processes for accessing proof of nationality	May be reluctant to apply for the ID for fear of being falsely identified as a non-national	

Group	Statutory	Procedural	Economic & Social	Technological
Refugees and asylum seekers	May not be included in the ID system	May have difficulty providing documentation or other evidence for identity proofing	May be reluctant to apply for fear of immigration enforcement or other negative consequences	
Stateless persons	May not be included in the ID system	May have difficulty providing documentation or other evidence for identity proofing	May be reluctant to apply for fear of immigration enforcement or other negative consequences	
Gender and sexual identity minorities	Laws and policies may prohibit (or make extremely difficult) changes in the gender/sex attribute of the ID system.	People may experience discrimination or persecution when attempting to register or update their gender in the ID system	People may fear persecution and discrimination when gender markers on their IDs do not match their physical presentation (e.g. in systems where gender is verified against a breeder document rather than self-reported)	Data standards may not allow for non-binary gender attributes
Poor people and rural dwellers	Penalties for late registration (e.g., of births) may be cost prohibitive	Complex registration requirements provide logistical and travel challenges	The direct and indirect costs (e.g., fees, travel, lost wages) to apply for or use the ID may be prohibitive	May lack smartphones or other resources to access online or digital services or use digital credentials (e.g., mobile ID)
Elderly people		Lack of mobility and/or accessible centers may hinder registration; the elderly also be more likely to lack certain identity documents (e.g., birth certificates) where these systems have been historically weak	The direct and indirect costs (e.g., fees, travel, lost wages) to apply for or use the ID may be prohibitive for many elderly people	May have difficult providing biometrics (e.g., fingerprints, iris scans); limited access/literacy to access digital services
Persons with disabilities		Lack of mobility and/or accessible centers may hinder registration, as may lack of trained staff and accommodating enrollment procedures	Stigma against persons with disabilities may prevent them from leaving home to enroll for IDs	May have difficult providing biometrics (e.g., fingerprints, iris scans, facial recognition)
Illiterate people		May have difficulty completing applications and/or confirming the accuracy of personal information in written form		May have difficulty remembering and using credentials such as ID numbers and PINs, and/or using advanced digital authentication technology

Once barriers have been identified, practitioners can adopt a variety of strategies to address these issues in system design and rollout. Mitigation efforts may involve adjustment to:

- The legal and regulatory framework
- Who is eligible to enroll in the ID system
- Whether and what types of biometrics are collected
- Whether and what types of sensitive information are collected
- Registration procedures and timelines
- Identity proofing requirements
- The types of credentials and authentication mechanisms adopted
- Communication campaigns
- Grievance redress mechanisms

3. KEY DECISIONS

After completing the analysis detailed in the Planning Roadmap, practitioners will have valuable information needed to make key decisions regarding the design of the ID system. This includes high-level policy and design decisions that will shape the overall architecture of the system and set the stage for the next level of technical specification and process design.

Table 18 summarizes these key decisions according to a variety of topics that are discussed in more detail in [Section III](#). Importantly, the order listed below is not meant to imply a sequence; these decisions are interdependent and should be made holistically.

Table 18. Examples of Key Decisions for ID systems

Section III. Topic	Key Decisions
Legal framework	Which policies, laws, and regulations need to be amended or updated to enable and safeguard the ID system? Which new policies, laws, and regulations are needed?
Public Engagement	How will the public be consulted during the planning phase and implementation? How will they be informed about the rollout and requirements of the ID system? How will the system correct errors and address grievances?
Administration	What will the institutional home, governance, and business model of the ID system be? What roles with the ID authority and other actors play (including the private sector) play?
Privacy & Security	What privacy- and security-enhancing technologies and operational controls will be built into the ID system from its inception to implement, enforce, and enhance the legal and management controls specified in the legal framework?
Data	What biographic data will be collected by the system? What (if any) biometric data will be collected?
IT Systems	Where will ID data be stored? What hardware, software, and applications will be used?
Registration & Coverage	Who will be eligible to enroll in the ID system? What strategies and timelines will be used for identity registration, updating, and outreach to vulnerable groups? How will identity proofing be carried out?
Credentials & Authentication	What structure will be used for unique ID numbers? What other types of credentials (if any) will be issued, and how? What authentication mechanisms will be adopted for different levels of assurance?
Interoperability	With which systems is the ID system required to interoperate, and how will interoperability be achieved? How will ID and CR systems be linked?
Standards	Which standards, including for technology, data, security, and more, will be used throughout the identity lifecycle?

4. PROCUREMENT

Transparent, competitive, and high-quality procurement practices are fundamental to overall project governance. Before preparing a request for proposals (RFP) for procurement of ID system components, countries should make key decisions and conduct a full needs assessment regarding the overall architecture of the ID system. After defining the enterprise and functional architecture of the system in accordance with these key decisions, practitioners should work to ensure that the procurement process meets internationally recognized good practices, particularly in terms of transparency and competition. This may include market consultations with the private sector to ensure that the RFP provides appropriate requirements that reflect the latest developments and practices.

In addition to transparency and good governance, procurement practices can also have a large impact on the overall cost of the system. As elaborated in the ID4D costing study, **the characteristics of the procurement process that may impact total cost include:**

- **Availability of in-house technical expertise:** Where the entity managing the ID system lacks sufficient in-house technical expertise, there may be a risk of procurement being heavily influenced by interested vendors, which could lead to higher program costs and potential vendor lock-in. As a risk mitigation measure, such countries could consider leveraging international technical expertise to provide inputs to the procurement process management, or a full-time program manager. In such cases, care should be taken to ensure that the consulting support is independent and not directly or indirectly influenced by or an extended arm of any potential bidders or future services providers. In addition, engaging international firms could also increase costs.
- **Vendor qualification process:** In cases where the vendor qualification criteria and process are limiting competition—e.g., sometimes driven by risk aversion or by other considerations—bidders can solicit higher premiums.
- **Over-specifying technical or process requirements:** Over-specification could lead to higher investments costs and may also limit the number of potential bidders. Instead, procurement should focus on functional requirements and outcomes, if the relevant procurement rules allow.
- **Appropriate use of international, open standards:** Using closed standards could impact the quality of supplies, premium pricing, and create vendor and/or technology lock-in.
- **Import restrictions and duties:** As in other projects that require the importation of technical infrastructure, restrictions on imports and duties will impact program cost. For example, the availability of biometric devices might be low in some countries and thus might require additional time to clear customs during delivery.

In addition, the *ID4D costing study* identified the following **good practices for procurement related to ID systems:**

- **Competition:** It is essential for governments to undertake an open and competitive procurement process that gives no special advantage to any specific vendor or set of vendors. The creation of competition will reduce costs and has potential to generate innovation in bids and proposals. In some cases—e.g., for niche applications or where innovative solutions are required to address specific needs or challenges—wide market adoption and competition will not necessarily exist. In such cases, it is vital to complete the additional steps below to avoid vendor and technology lock-in.
- **Government ownership:** It is critical to have a procurement model which allows for ownership over data, as well as facilitation of seamless transfer of system management and services to alternative providers. Government should have access to the software source code.
- **Specifying ongoing service agreements:** Embedding the right technical support requirements from vendors in the initial contract is an important procurement consideration, as surprise fees for later maintenance can be very costly. This should include the end-of-life service to support transfer of the system and data to other parties in case the contract is terminated.
- **Performance-linked procurement models:** Outcome-based contracts (e.g., for private enrollment agencies in India) can be an efficient way to bringing greater vendor accountability and maximize the use of external program resources.
- **Open-technology and data portability (e.g., open source software and open APIs):** Opting for an open-technology interfaces will allow governments enough flexibility to easily upgrade critical system components with minimal vendor dependency, minimizing longer term costs. In addition, ensuring data portability from one system to the next will help prevent vendor lock-in.
- **Connecting internationally recognized good practices with local knowledge:** Promote the transfer of international know-how and good practices by encouraging the participation of local firms, e.g. through joint venture or subcontracting arrangements.

When preparing the RFP, countries should—at a minimum—complete the RFP checklist detailed in Box 6.

Box 6. RFP Checklist

- ✓ Is the RFP based on the desired functional requirements and outcomes of the ID system?
- ✓ Are the qualification criteria and functional requirements vendor-neutral and do they allow all possible service providers to participate?
- ✓ Does the RFP insist on the use of open standards for IT devices, software, and services?
- ✓ Does the RFP limit the use of proprietary software solution except in very limited and specified cases like ABIS? [Even in such cases the solution proposed should provide for enabling mechanism (technical, commercial and contractual) for replacement of such proprietary solutions.]
- ✓ Does the RFP specify conditions for exit & transition management?
- ✓ Does the RFP provide for clearly articulated service-level agreements (SLAs), including for warranty and maintenance services, measurement of performance against SLAs, and preferences for various design choices?
- ✓ Does the RFP cover the intellectual property rights (IPR) and license agreements as applicable?
- ✓ Does the RFP cover provisions based on the cybersecurity strategy and plan?










Source: Adapted from *ID4D Costing Study*

Box 7. Planning Tools

For more planning resources that can assist with decision-making, see:

- [Guidelines for ID4D Diagnostics](#) and completed [ID4D Diagnostics](#)
- [ID Enabling Environment Assessment \(IDEEA\)](#)
- [Technology Landscape for Digital Development](#)
- [Catalog of Technical Standards for Digital Identification Systems](#)
- [Understanding Cost Drivers of Identification Systems](#) and [Cost of Identification Systems: Reference Cost Model](#)
- [Public Sector Savings and Revenue from Identification Systems](#)
- [Private Sector Economic Impacts from Identification Systems](#)
- [Digital Identity Toolkit](#)
- Procurement checklist (*pre-publication*)

SECTION III. Topics

 TOPICS	 Legal Framework Policies, laws, and regulations to support an inclusive, robust, and responsible ID system	 Public Engagement Public consultation, communication campaigns, and grievance redressal	 Privacy & Security Operational and technical controls for a privacy-and-security-by-design approach to ID	 Administration Institutional arrangements, governance, and business models of a foundational ID authority	 Data Biographic and biometric attributes collected for the ID system
	 IT Systems IT systems, applications, and infrastructure, including data storage, hardware, and software	 Registration & Coverage Eligibility, enrollment strategies and equipment, and identity proofing	 Credentials & Authentication Types of credentials, issuing, authentication, levels of assurance	 Interoperability Frameworks, links with civil registration, data exchange & APIs, mutual recognition across borders	 Standards Technical and data standards

To make the key decisions described in Section II, practitioners need to know the best-practice options that are available. This section provides more detailed information about design choices, organized according to topic. In addition to providing more technical information, it also discusses the implications of design choices for the system’s adherence to the *Principles*, particularly with regard to inclusivity, trustworthiness, data protection, and sustainability. Note that the order in which these topics are presented is not meant to imply a sequence or relative level of importance; each of these topics are interrelated and should be considered holistically.

Contents:

- [Legal Framework](#)
- [Public Engagement](#)
- [Privacy & Security](#)
- [Administration](#)
- [Data](#)
- [IT Systems](#)
- [Registration & Coverage](#)
- [Credentials & Authentication](#)
- [Interoperability](#)
- [Standards](#)

LEGAL FRAMEWORK

ID systems must be built on a foundation of trust and accountability between government agencies, individuals, international organizations, and the private sector, both within countries and across borders. A cornerstone of this foundation are the laws, codes, regulations, and practices that govern and support the ID system—i.e., the “legal framework.”

In some countries, legal frameworks and practices may already enable inclusive and trusted ID systems. In many other cases, however, key laws and regulations do not exist, are not enforced, do not comply with international law, or predate the use of digital ID systems and trust services such as electronic signatures. A thorough assessment (e.g., using the *IDEEA*) during the planning stage will help identify areas in which the legal framework may need to be amended, or updated.

In general, the policies, laws, and regulations that support an ID system can be divided into two categories:

1. **Enablers**—directly define and govern the ID system, including its design, management, operation, and relationships with stakeholders and other systems.
2. **Safeguards**—address potential risks surrounding the ID system, including those related to data privacy, security, and non-discrimination.

The particular architecture of the enablers and safeguards that make up a legal framework for ID will vary by country, and there is no one blueprint model. However, this section highlights some important areas and themes that should be covered as part of a comprehensive legal framework on identification (as enshrined in Principles 8, 9 and 10, see *Section II. Principles*). For a more detailed treatment of legal and regulatory frameworks, see the IDEEA.

Enablers

A comprehensive legal framework begins with policies, legislation, and regulations to define and govern the ID system, including its mandate, design, institutions, characteristics, relationships, accountabilities, oversight, and more. Given the specificity of enabling legislation to the country and legal context, it is not possible to enumerate all possible aspects or features to be addressed by such policies, laws and regulations here. However, many of the policy choices enumerated in *Section II. Key Decisions* will need to be supported by—or reflected in—the legal framework. These could include, but are not limited to:

- The scope and purpose of the ID system (e.g., that the purpose of the ID to provide a foundational, universal digital identity)
- Eligibility requirements for registration in the ID system (e.g., that it is open to all ages and not linked to nationality)



- System specifications (e.g., that it will involve the establishment of a population register with a unique, random identifier, which data will be collected, etc.)
- The creation, mandate, independence, and budget of the entity that oversees the ID system
- The operation and staffing of this authority, including the selection criteria for and terms and conditions of appointments, as well as dismissal of key employees
- The form, role, and process of appointments of any governance mechanisms (e.g., a board)
- The Interoperability of the ID system with other systems (e.g., the civil register, other government systems, and private sector actors)
- Data sharing and transfer policies
- Grievance redress mechanisms
- The mutual recognition of the ID within the country and across borders
- Whether the ID system will be bound by open standards and technology neutrality

In particular, creating a coherent and trusted ID system with wide coverage requires an overarching legal and policy framework that provides transparent and comprehensive institutional mandates and accountability. The **role of each actor in the identity ecosystem should be clear and publicly available, as should responsibilities within each institution**. Identity providers should establish memoranda of understanding (MOUs) or equivalent with other agencies for the exchange and use of data and for authentication and verification services.

Safeguards

The “safeguards” portions of the legal framework generally seek to mitigate the risks of an ID system, including those related to data privacy and protection, cybersecurity, and non-exclusion and non-discrimination. This section provides examples of the types of laws, regulations, and policies in these three categories and the kinds of safeguards they should or might include.

Data protection and privacy laws

As described in **Section III. Privacy & Security**, data protection requires a holistic approach to system design that incorporates a combination of legal, administrative, and technical safeguards. To begin, ID systems should be underpinned by legal frameworks that safeguard individual data, privacy, and user rights. Many countries have adopted general data protection and privacy laws that apply not only to the ID system, but to other government or private-sector activities that involve the processing of personal data. In accordance with international standards on privacy and data protection (see Box 8Box 8. EU General Data Protection Regulation (GDPR)), these laws typically have broad provisions and principles specific to the collection, storage and use of personal information, including:

- **Purpose limitation.** The collection and use of personal data should be limited to purposes: (1) which are stated in law and thus can be known (at least in theory) to the individual at the time of the data collection; or (2) for which the individual has given consent.
- **Proportionality and minimization.** The data collected must be *proportionate to the purpose* of the ID system in order to avoid unnecessary data collection and “function creep,” both of which can create privacy risks. This is often articulated as requiring that only the “minimum necessary” data—including transaction metadata—should be collected to fulfil the intended purpose.
- **Lawfulness.** The collection and use of personal data should be done on a lawful basis, e.g., involving consent, contractual necessity, compliance with legal obligation, protection of vital interests, public interest and/or legitimate interest.
- **Fairness and transparency.** The collection and use of personal data should be done fairly and transparently.
- **Accuracy.** Personal data should be accurate and up-to-date, and inaccuracies should be expediently corrected.
- **Storage limitations.** Personal data—including transaction metadata—should not be kept longer than is necessary for the purposes for which it is collected and processed. With respect to transaction metadata, people can be given an option for how long such data are retained.
- **Privacy-enhancing technologies (PETs).** Requirements to use technologies that protect privacy (e.g., the tokenization of unique identity numbers) by eliminating or reducing the collection of personal data, preventing unnecessary or undesired processing of personal data, and facilitating compliance with data protection rules.
- **Accountability.** The processing of personal data in accordance with the above principles should be monitored by an appropriate, independent oversight authority, and by data subjects themselves.

In general, personal information should be lawfully obtained (usually through freely given consent) for a specific purpose, and not be used for unauthorized surveillance or profiling by governments or third parties or used for unconnected purposes without consent (unless otherwise required under the law). Finally, users should have certain rights over data about them, including the ability to obtain and correct erroneous data about them, and to have mechanisms to seek redress to secure these rights.

The sections below describe some particular data protection safeguards in relation to institutional oversight, data security, data sharing, cross-border data transfers, and user consent.

Box 8. EU General Data Protection Regulation (GDPR)

In terms of existing frameworks, the **European Union's (EU)** 2016 *General Data Protection Regulation (GDPR)* is the most recent example of comprehensive regulation of data protection and privacy, setting a new threshold for international good practices. Building upon existing principles (e.g., the OECD Privacy Principles), it has become an important reference point for global work in this area. Article 5 of the GDPR, enshrines the core principles described above, requiring that personal data collection, storage, and use be:

- processed lawfully, fairly and in a transparent manner in relation to the data subject;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- accurate and, where necessary, kept up to date;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and
- processed in a manner that ensures appropriate security of the personal data.

In addition, EU Member States are required to provide for a supervisory authority to monitor the application of the regulation (Article 51(1)). However, many Member States had previously established their own supervisory authorities under the EU Data Protection Directive (Directive 95/46/EU); the incumbent EU data protection regime.

Some of the newer rights and duties it introduced when the GDPR took force in 2018 remain the subject of debate in policy circles, and a number of legal questions remain about their application in practice. However, the framework's key principles largely have their origins in earlier European law and are not new or specific to Europe or the GDPR. They are reflected in one form or another in many national data protection and privacy laws outside Europe, largely due to general recognition of their merit.

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

Institutional oversight

Data protection and privacy in general, and with respect to ID systems, are often subject to the oversight of an independent supervisory or regulatory authority to ensure compliance with privacy and data protection law, including protecting individuals' rights. The supervisory authority might be a single government official, ombudsman or a body with several members. Genuine independence of such an authority is a key factor, with independence being measured by structural factors such as the composition of the authority, the method of appointment of members, the power and timeframe for exercising oversight functions, the allocation of sufficient resources and the ability to make meaningful decisions without external interference (e.g., see Recital 117 of the *GDPR*).

The supervisory authority may handle public complaints, even though every individual whose data is collected may have recourse to an external binding legal process and ultimately the courts at least on matters of law. In terms of remedies, the authority may have the power to oblige the ID system to rectify, delete or destroy inaccurate or illegally collected data.

Specifically, the Council of Europe (CoE) *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108, *CoE 2018*)—which was recently updated as Convention 108+—indicates that **the powers and duties of such an authority may include:**

- duties to monitor, investigate and enforce compliance with individual privacy and data protection rights;
- duties to monitor developments and their impact on individual privacy and data protection rights;
- powers to receive complaints and conduct investigations of potential violations of individual privacy and data protection rights;
- powers to issue decisions on violations of such rights and order remedial action or meaningful sanctions;
- duties to promote public awareness of the rights of individuals and the responsibilities of those entities holding and processing personal data; and
- a duty to give specific attention to the data protection rights of children and other vulnerable individuals.

The CoE has further suggested that a supervisory authority might also have other powers and duties, such as:

- issuing opinions prior to the implementation of data processing operations;
- advising on legislative or administrative measures;
- recommending codes of conduct or referring cases to national parliaments or other state institutions;
- issuing regular reports, publishing opinions and other public communications to keep the public informed about their rights and obligations and about data protection issues in general.

Box 9. Examples of data privacy and protection oversight agencies

The **Estonian Data Protection Inspectorate**, founded in 1999, is a supervisory authority, empowered by the Data Protection Act, Public Information Act and Electronic Communication Act. The inspectorate's mandate is to protect the following right enshrined under the Estonian Constitution:

- right to obtain information about the activities of public authorities;
- right to inviolability of private and family life in the use of personal data; and
- right to access data gathered in regard to yourself

In **South Africa**, the Protection of Personal Information Act 4 of 2013 established the Information Regulator, an independent body subject only to the Constitution and to the law. This body is appointed by the President on the recommendation of the National Assembly, after nomination by a committee composed of members of all the political parties represented in the National Assembly. It is ultimately accountable to the National Assembly. It has a broad range of supervisory functions, including a duty to: conduct public education, monitor and enforce compliance with the law, consult stakeholders and mediate between opposing parties, handle individual complaints, conduct relevant research, issue codes of conduct and guidelines, and facilitate cross-border cooperation. Among its monitoring functions are the periodic assessment and monitoring of public and private bodies engaged in processing of personal data and monitoring the use of unique identifiers of data subjects. Note that as of August 2018, the Act has not yet been brought fully into force.

In the Philippines, the Data Privacy Act of 2012 established the independent National Privacy Commission. The Commission, which is attached to the Department of Information and Communications Technology, is headed by a Privacy Commissioner who is assisted by two Deputy Privacy Commissioners (one responsible for Data Processing Systems and one responsible for Policies and Planning). All three Privacy Commissioners must be expert in the field of information technology and data privacy, and all are appointed by the President for three-year terms and are eligible for reappointment for a second term of office. The Commission has its own secretariat. The Commission's many duties include monitoring compliance with the data privacy law; receiving and investigating complaints; regularly publishing a guide to all laws relating to data protection; reviewing and approving privacy codes voluntarily adopted by personal information controllers; providing opinions on the data privacy implications of proposed national or local statutes, regulations or procedures; and coordinating with data privacy regulators in other countries (See Philippines Data Privacy Act of 2012, Chapter II.)

In the **United Kingdom**, the Data Protection Act 1984 introduced the role of Information Commissioner (previously, the Data Protection Registrar) although the powers granted to the Information Commissioner increased in scope under the Data Protection Act 1998 and most recently, the Data Protection Act 2018. The Information Commissioner is an independent official appointed by the Crown and operates the UK Information Commissioner's Office (ICO). The ICO is sponsored by the Department for Digital, Culture, Media and Sport (DCMS) and ultimately reports to Parliament. It is an independent regulatory body which seeks to monitor, investigate and enforce all applicable data protection and privacy legislation in the UK (including Scotland, to a limited extent).

Source: Adapted from *ID Enabling Environment Assessment (IDEEA)* and *Privacy by Design: Current Practices in Estonia, India, and Austria*

Data security

Personal information should be stored and processed securely and protected against unauthorized or unlawful processing, loss, theft, destruction, or damage. This principle becomes increasingly important for digital ID systems given the threat of cyberattacks. Typical measures to

ensure data security that may be mandated under the legal framework—some of which are discussed in more detail under *Section III. Privacy & Security*—include:

- Encryption of personal data
- Anonymization of personal data
- Pseudonymization of personal data
- Confidentiality of data and systems that use or generate personal data
- Integrity of data and systems that use or generate personal data
- Ability to restore data and systems that use or generate personal data after a physical or technical incident
- Ongoing tests, assessments and evaluation of security of systems that use or generate personal data

Many international standards also **impose a duty on data controllers to notify data subjects of significant** data breaches **affecting their personal data**. In addition, countries may have laws designed to identify and mitigate cyberthreats, as well as legislation that penalizes unauthorized access, use or alteration of data (see section on Cybersecurity, below). Finally, legal frameworks should include **sufficient penalties for unauthorized access, use or alteration to personal data** by data administrators and third parties, including the criminalization of:

- Unauthorized access to ID systems or other databases holding personal data
- Unauthorized monitoring/surveillance of ID systems or other databases holding personal data or unauthorized use of personal data
- Unauthorized alteration of data collected or stored as part of ID systems or other databases holding personal data
- Unauthorized interference with ID systems or other databases holding personal data

Box 10. Examples of security breach notification laws

The **EU's** GDPR requires notification to the supervisory authority of any personal data breach “without undue delay and, where feasible,” within 72 hours of becoming aware of it unless the incident “is unlikely to result in a risk to the rights and freedoms of natural persons.” The notification must detail certain information about the breach including the categories and approximate number of data subjects concerned and the likely consequences of the breach (Article 33). Similarly, subject to some exceptions, notification to the individual data subjects affected must take place “without undue delay” if the breach “is likely to result in a high risk to the rights and freedoms of natural persons” and such notification shall have at least the same information that needs to be notified to the supervisory authority (article 34).

Almost every state in the **United States** has a breach notification statute, typically requiring private or governmental entities to notify individuals of security breaches involving personally identifiable data and setting out what constitutes a security breach, notice requirements (such as timing and method), and exemptions (such as for encrypted information) (see <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>).

In **South Africa**, the Protection of Personal Information Act 4 of 2013 (most of which was not yet in force as of August 2018) requires the Information Regulator, the national supervisory authority, to notify the data subjects of breaches as soon as reasonably possible after their discovery of the compromise – taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party’s information system. The notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the data breach including. The Information Regulator may direct the responsible party to publicize information about the security breach if this would protect individuals who may be affected (South Africa Protection of Personal Information Act 4 of 2013, section 22).

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

Data sharing

Because the linkage of information across databases intensifies privacy and data protection concerns, legal frameworks can **mitigate risks by stipulating all the purposes for which personal data in an ID system is shared, by both government and non-government entities**. In addition, public entities may be limited to obtaining specific information justified by their functions (i.e., the “need-to-know” principle).

Potential benefits of information sharing include:

- convenience for both government and citizen;
- better government service delivery;
- seamless service transfer when data subjects change address;
- improved risk management;
- cost savings as duplication of effort is eliminated; and
- improved efficiency through more effective use of data (see, e.g., *Perrin et al. 2015*)

However, information-sharing between government agencies, if not well-regulated, can turn into a “back door” which allows circumvention of individual privacy and data protection safeguards. Comprehensive population databases, like those established as part of ID systems, are a tempting resource for law enforcement authorities, particularly when they contain biometrics. Particular concerns arise in relation to collection of DNA information which, like other biometric data, may be

used not only for the purposes of identifying an individual, but also as evidence in the process of investigating whether he or she has committed a crime.

This type of information sharing can take place even without the technological compatibility of interoperability. For example, police could contact ID officials and ask them to pull the record of a particular individual and share information such as fingerprints, facial image, address or names of family members.

Policymakers and courts have struggled with striking the appropriate balance between protecting the privacy of registrants and supporting criminal investigations. One approach to such matters could be to apply the same rules that apply to other forms of searches and seizures in the country in question, such as a requirement that a warrant be obtained. This may be beneficial where a balance between personal privacy and public interest has already been struck in this regard. For further discussion and citations on this issue in scholarly work and the media, see the *IDEEA tool*.

Box 11. Examples of data sharing arrangements

Article 4(2) of the **EU** 2016 *Police and Criminal Justice Data Protection Directive 2016/680* requires that personal data collected for some other purpose—which could be for an ID system or for civil registration—can be processed by the same or another controller for crime-related purposes *only* in so far as: (a) there is legal authorization for this *and* (b) such processing is necessary and proportionate to the purpose for which the personal data was collected. (See, e.g., <https://www.consilium.europa.eu/en/policies/data-protection-reform/data-protection-law-enforcement/>)

In **India**, the *Aadhaar Act 2016* provides for the disclosure of information, excluding “core biometric information,” pursuant to an appropriate court order, which can be made only after the Unique Identification Authority of India (UIDAI) has been given an opportunity to give input on the disclosure. It also provides for the disclosure of information, including core biometric information, “in the interest of national security” on the direction of government officers above a certain rank, where this has been authorized by an order of the central government and reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government in the Department of Legal Affairs and the Department of Electronics and Information Technology.

In **Australia**, the federal *Privacy Act 1988* (as amended) contains as one of its “Privacy Principles” the rule that personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual’s consent. However, there is an exception for situations where the use or disclosure is “reasonably necessary” for the enforcement related activities conducted by or on behalf of an enforcement body – which includes use or disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences – as well as an exception for uses and disclosures authorized by law or by court order. Use for enforcement related activities must be noted in writing as a mechanism to promote accountability. (See also https://www.agps.gov.au/publications/fact-sheets/Fact_sheet_No_27.pdf)

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

Cross-border data transfers

The security of personal data transferred across national borders has been one of the drivers for international consensus on the fundamental principles for the protection of personal data. For example, the principle articulated in the OECD Privacy Framework (*OECD 2013*) regarding transborder flows of personal data is that a data controller “remains accountable for personal data

under its control without regard to the location of the data” (adopted in 1980 and revised in 2013, Article 17).

However, due to uncertainty regarding data protection standards in foreign countries, many countries limit extraterritorial transfer of personal data. Such transfers may be permitted in certain circumstances or when the data protection standards in a third country are deemed adequate. This is particularly sensitive in the case of personal data for national ID systems, civil registration, and voter registration systems. In addition to transferring data across borders, legal frameworks may also include arrangements for regional or international interoperability or mutual recognition of their ID systems.

Box 12. GDPR limits on data transfers

The **EU's** GDPR limits transfers of personal data outside the European Economic Area except in certain circumstances. Such transfers are allowed if the European Commission issues a decision determining that the receiving country “ensures an adequate level of protection” (Article 45). Such a decision requires a comprehensive assessment of the country’s data protection framework, including protections applicable to personal data and oversight and redress mechanisms. Adequacy decisions have been adopted with respect to 12 countries, including Canada (commercial organizations), Israel, Switzerland and the United States (limited to the Privacy Shield framework). (See https://europa.eu/rapid/press-release_MEMO-18-4503_en.htm).

In July 2018, the EU and Japan agreed to recognize each other’s data protection system as equivalent, and the European Commission began the process of formally issuing an adequacy decision. Similarly, the United Kingdom is seeking to obtain an adequacy decision from the European Commission to apply upon the UK’s exit from the European Union (Brexit). Transfers to non-EU countries are also permitted in other circumstances, such as if the transferor has provided “appropriate safeguards” which may be established through several means including a legally binding agreement between public authorities, certain contractual clauses (e.g. the EU Commission’s Model Clauses) or the existence of an approved and enforceable code of conduct, among others (GDPR Article 46).

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

User consent and control

One widely accepted privacy principle is that an **individual’s personal data should only be collected and used with the consent of that individual** unless there is another basis in law for such collection and use (see Annex II of the *IDEEA Guidance Note*). Where consent is the basis for collection, transparent disclosure to the individual of the nature of his/her personal data collected and the intended uses of such data is essential for consent to be meaningful.

Many international and regional standards and national laws make exceptions to the consent requirement for collection and use of personal information where government collects data pursuant to legal authority, such as data collected for ID systems (see, for example, the EU Commission’s model contracts for international data transfers). Where no consent is required or obtained, transparency can at least provide clear and accessible explanations to assure public trust and prevent misconceptions. Individuals can be informed of which information is considered public and which will remain confidential.

Some countries use a “privacy policy” in the form of to an easy-to-understand document which explains in plain language how personal information is collected and used. However, public awareness campaigns are also crucial to disseminate information on the collection and use of personal data. These can address misconceptions and concerns and identify channels for questions and complaints.

Box 13. Examples of user consent laws

Where the personal data being processed is special category data (for example, biometric data), The **EU’s** GDPR specifies that additional conditions must be satisfied, one of which is obtaining the individual’s “explicit” consent to the processing (GDPR Article 9). It is not clear whether there is a difference between standard consent and explicit consent (since standard consent must be specific, informed and affirmative action). However, given the GDPR has only been implemented recently it is likely that further guidance will be issued to clarify this.

The **California** *Consumer Privacy Act of 2018* applies to certain businesses that collect personal information of California residents and will go into effect in 2020. The Act, unlike the GDPR, does not strictly require consent prior to collection of personal information, in most cases. However, at the point of information collection, consumers must receive notice “as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used” (Cal. Cov. Code §178.100(b). Additional information must be disclosed in an online privacy policy or a website and updated every 12 months (Cal. Cov. Code §178.130(a).

In **Australia**, the federal *Privacy Act 1988* (as amended) contains as one of its “Privacy Principles” the rule that personal information about an individual collected for a particular purpose must not be used or disclosed for another purpose without the individual’s consent. However, there is an exception for situations where the use or disclosure is “reasonably necessary” for the enforcement related activities conducted by or on behalf of an enforcement body—which includes use or disclosure by police for prevention, detection, investigation, prosecution or punishment of criminal offences—as well as an exception for uses and disclosures authorized by law or by court order. Use for enforcement related activities must be noted in writing as a mechanism to promote accountability. (See Section 6 of the Privacy Act, Schedule 1 clause 6 of the Australian Privacy Principles, and also https://www.agps.gov.au/publications/fact-sheets/Fact_sheet_No_27.pdf.

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

In addition to user consent, many legal and regulatory frameworks—including the OECD Privacy Framework, Chapter 3 (**OECD 2013**) and International Covenant on Civil and Political Rights, General Comment 16 on Article 17 (**UN 1988**), the *Council of Europe’s* Convention 108+ (**CoE 2018**), and the APEC Privacy Framework, Article 23c (**APEC 2004**)—include **the rights of individuals to access, review, rectify and erase personal data about them**. Even in a mandatory ID scheme, the “right of erasure” or “right to be forgotten” could arise in respect to specific aspects of personal data, such as biometric data (particularly genetic material), a previous married surname, or the names of the birth parents of an adopted child (see, for example, *Kelly & Satola 2017*, *Kindt 2013*, *Chadwick 2014*). Legal measures that ensure the right to access, review, correct, and erase personal data should be put into practice through clear administrative procedures and technical measures for personal oversight and grievance redress.

Finally, **some legal and regulatory frameworks guarantee data portability as an individual right**. Data portability refers to the ability to easily move, copy or transfer personal data about an individual from one technological environment to another. This portability allows individuals to utilize the

collected data in other contexts. With respect to commercial enterprises, such portability mitigates the risks of consumers becoming locked into a single service provider that would otherwise have an advantage over competitors which did not have ready access to such data. In terms of an ID system, such a right potentially enables individuals to use personal data collected by the system for other technological applications, preventing consumer “lock in” to services.

Cybercrime and cybersecurity

For each kind of crime in the analog world, there is an equivalent in the digital world. For instance, theft of property or identity can occur digitally. Hostage taking, ransom holding, attacks on critical infrastructure—these occurrences that amount to crime in the real world have a cybercrime parallel in the virtual world.

Cybercrime laws provide enforcement powers against such violations. Cybercrime may have a wide range of meanings depending on the country, legal instrument and context in which the phrase is used, but in general a country should have laws in place addressing criminal conduct—as provided in the country’s criminal laws—directed against the confidentiality, integrity and availability of computer systems and networks, as well as the data stored and processed on them, and criminal acts carried out through the instrumentality of such systems, networks, and data. This broad approach to the definition of cybercrime is drawn from the World Bank Toolkit on Combatting Cybercrime (*World Bank 2017*, available at <http://www.combattingcybercrime.org>).

Typically, a cybercrime law will criminalize unauthorized access, use or alteration to personal data or ID systems, including the criminalization of:

- Unauthorized access to ID systems or other databases holding personal data
- Unauthorized monitoring/surveillance of ID systems or other databases holding personal data or unauthorized use of personal data
- Unauthorized alteration of data collected or stored as part of ID systems or other databases holding personal data
- Unauthorized interference with ID systems or other databases holding personal data

Good practices include:

- Considering maintaining separate laws for cybersecurity and cybercrime. In some countries, cybercrime legislation does not provide sufficient coverage for cybersecurity measures. If the laws are combined, ensuring that cybersecurity of national critical information infrastructure is comprehensively covered and maintained.
- Clearly stating the penalties for cybercrime violations but also for breach of obligations by critical national infrastructure holders.
- Defining a timeline for reporting cybersecurity incidents to the authorities
- Establishing clear powers for a computer emergency response teams (CERT) to prevent and investigate cybersecurity breaches
- Establishing clear powers for a Ministry of Justice’s cybercrime Prosecution unit

- Considering provisions requiring cybersecurity service providers and products to be licensed and auditable.
- Establishing a legal framework that sets standard for IT security of government information system and databases and their auditing.

Non-exclusion and non-discrimination

Some aspects of universality can be addressed in the enabling legislation, but here, the focus is on ensuring that the ID system is not discriminatory or exclusive. In that sense, ID systems should not exclude linguistic, ethnic, religious or other vulnerable groups. Furthermore, the country's identity ecosystem should cover both citizens and residents.

Multiple constitutional provisions, laws, international conventions, regulations, and policies have the potential to impact the inclusivity of the ID system, including many of the ID system enabling laws. This includes, for example, those related to:

- The mandatory nature of the ID system
- Who is eligible for the ID system, including citizens and non-citizens, children and adults
- The definition and determination of nationality and legal status
- The collection of sensitive biographic information and biometrics
- Non-discrimination and protection of minorities (e.g., based on gender, race, ethnicity, religions, disability, etc.)
- Migrants
- Refugees
- Stateless populations
- Fees charged for ID services
- Required identity evidence for enrollment (e.g., requiring proof of citizenship)

Such policies, laws, and regulations can therefore *directly* or *indirectly* affect the exclusion and/or targeted discrimination of multiple groups, including:

- Individuals who do not speak an official language
- Racial, ethnic, or religious groups
- Women and girls
- Persons with disabilities
- The elderly
- Individuals in remote or inaccessible areas
- Undocumented adults
- Undocumented children, or children of undocumented adults
- Refugees
- Migrants
- Stateless persons
- Gender and sexual minorities
- Neglected, abandoned, or orphaned children
- The mentally ill
- Others

To ensure universal coverage of the ID system, the legal framework should therefore be updated to remove or amend the above laws to excise explicit instances of discrimination and other barriers to access. Practitioners should also ensure compliance with international norms and conventions that enshrine the right to recognition before the law and require governments to provide every refugee, stateless person, and internally displaced person with a means of identifying themselves (e.g., in the form of passports, identity documents, birth certificates, etc.), including the UN Convention relating to the Status of Refugees (Article 27), the Convention relating to the Status of Stateless Persons (Article 27), the *UN Guiding Principles on Internally Displaced Persons* (Principle 20), and the Convention for the Protection and Assistance of Internally Displaced Persons in Africa (Article 13).

In addition to the above, practitioners should pay special attention to policies, laws, and regulations related to design-features of the ID system that have the potential to exclude significant portions of the population. This includes whether or not the ID is mandatory, which is discussed below, and topics discussed in a variety of other sections in this Guide, including who is eligible to register in the ID system (including citizens and non-citizens), which data are collected, registration procedures and strategies, what technology is used for credentials and authentication, mechanisms for public engagement, and more.

Box 14. Examples of legal measures for inclusion

In some countries, inclusion efforts are built into the legal framework for ID. In **India**, for example, the Aadhaar Act calls for special measures to ensure the inclusion of women, children, senior citizens, persons with disabilities, unskilled and unorganized workers, nomadic tribes and other categories of individuals as may be specified by regulations (Aadhaar Act 18 of 2016, §5).

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

Mandatory nature of ID

Some countries have ID systems that are explicitly mandatory, in the sense that the law imposes a sanction for failure to enroll. However, even where the ID system is ostensibly “voluntary,” it may become mandatory *in practice* if it is required to access to services and other transactions, making it impractical for anyone to opt out.

A strict conditioning of essential government services on the presentation of a specific ID can be problematic if access to that ID system is not universal or is applied in discriminatory ways. This problem can be particularly acute when IDs are required for services (like financial services that require KYC) but are provided *only* to nationals, unless alternative means are made for residents and other groups ordinarily living in a country—e.g., migrants, refugees, and stateless persons—to access public and private sector services. A number of jurisdictions have seen legal challenges to the constitutionality of mandatory ID systems, including India, Jamaica, and Kenya. In the United States, for example, certain religious groups challenged the requirement to obtain a social security number and were exempted (see <https://secure.ssa.gov/poms.nsf/lnx/0110225035>).

In addition, some countries make it compulsory for people to carry physical identity credentials with them at all times and impose fines or other sanctions for failure to do so. Such systems have been criticized on the grounds that they create too many openings for abuse. Demanding that credentials be shown can be an avenue for police harassment of minority groups or persons who appear

“foreign” and so are suspected of being undocumented immigrants, as well as serving as a prelude to more intrusive searches or investigations. It may also make people unnecessarily fearful of a situation where their ID credential is lost, stolen or destroyed. The mere fact of having to prove identity in a public space for no particular purpose may impinge on an individual’s privacy—such as laws applied in apartheid South Africa. However, public attitudes about requirements such as these may vary depending on the local legal and cultural attitudes.

Box 15. Additional resources on legal frameworks

For more on legal and regulatory frameworks, see

- [ID Enabling Environment Assessment \(IDEEA\)](#)
- [Guidelines for ID4D Diagnostics](#)

PUBLIC ENGAGEMENT





People are at the heart of ID systems—yet many identification projects are launched without significant public involvement during the planning stage or throughout the identity lifecycle. As both the subjects and end-users of identification, people’s participation in and knowledge of ID systems must be a priority for the system’s success.

Primary decisions regarding public engagement include:

- What consultative processes will be used to understand people’s needs, concerns, and expectations regarding identification and to identify potential barriers to registration and use?
- What communication and education strategies will be adopted?
- What grievance redress mechanisms will be put into place?

Where ID providers fail to understand people’s needs and attitudes regarding identification—and the barriers they face in terms of registration—coverage is likely to be low. Similarly, robust information and education campaigns, ongoing feedback during implementation, and sensible grievance redress mechanisms are needed to build trust in the system and help people take advantage of the opportunities it can provide, as shown in Figure 11. Transparent and frequent involvement with civil society and community-based organizations—particularly those that represent the interests of marginalized and vulnerable groups—can help facilitate public engagement at all stages of project planning and implementation.

Figure 11. Key considerations for public engagement

 Inclusion	 Reliability	 Data Protection	 Sustainability
When done well, public engagement can help identify and mitigate barriers to inclusion ; when done poorly, it can fuel mistrust or apathy toward the system.	Intuitive and accessible grievance redress mechanisms to correct and update data are essential for maintaining the integrity of data .	Ongoing engagement in response to real or perceived privacy risks to the system are necessary to address threats and foster trust in the system .	Public consultation <i>before</i> implementation can help calibrate system design to the current and future needs of the public— avoiding investments in systems that are not fit-for-purpose .

Public consultation

For an ID system to be successful, the population—including vulnerable groups—must have trust and confidence in its design and implementation, particularly with respect to the collection, use and protection of sensitive personal data. For example, the population may perceive that an ID system is motivated by a Government’s desire to carry out mass surveillance. Building trust and confidence begins with understanding people’s perspectives on identification and privacy.

Furthermore, gaining first-hand knowledge of people's struggles and hopes for the ID system will help reduce exclusion by providing critical input necessary to remove barriers to access. Additionally, consultation can help **surface issues with implementation** that allow practitioners to maximize the effectiveness of the system.

Public consultation should not be a one-off activity—rather, it should begin during the planning phase and continue throughout the project. Different methods of consultation are shown in Table 19. For more guidance, ID4D has a forthcoming toolkit on qualitative end-user research.

Table 19. Potential methods of public consultation

Method	Benefits
End-user research	<p>End-user research can include both quantitative data collection (e.g., surveys) and qualitative methods, including focus group discussions, interviews, and interactive exercises.</p> <p>When conducted early-on in a project, end-user research can help surface people's perceptions, understanding, struggles, and needs regarding identification. This information can provide critical input to help shape the design and implementation of the system, including registration strategies, credential formats, authentication mechanisms, use cases for the ID, and communication efforts. In particular, end-user research that focuses on or includes marginalized groups is essential for mitigating the risk of exclusion and building trusted ID systems.</p> <p>Ongoing end-user research throughout the life of the project—or when rolling out new features—can similarly help surface issues with implementation or help inform later reforms.</p>
Standing civil society committee	<p>ID authorities can benefit from establishing a committee of civil society representatives that can provide feedback on the design of the ID system and on implementation of the system throughout the identity lifecycle. Members of the committee can utilize social accountability mechanisms (e.g., third-party monitoring, beneficiary scorecards, etc.) to monitor and report on critical issues related to all part of the identity lifecycle – from awareness raising and communications to enrollment to authentication. Civil society can also be critical to surfacing issues from marginalized communities who do not engage with the ID system and whose feedback would not otherwise be captured.</p>
Regular public consultation meetings	<p>ID authorities should regularly consult with the public on emerging trends and challenges that are surfaced by civil society or through grievance redress mechanisms. Regular consultation workshops or meetings with different target groups or in different cities can give the practitioners the opportunity to hear from beneficiaries about the challenges arising from the ID system.</p> <p>A regular schedule of consultations (e.g., quarterly, bi-annual, or annual) gives the authority the opportunity to close the feedback loop between beneficiaries and government by reporting back on actions taken to address previous concerns and grievances and to seek additional civil society and beneficiary feedback.</p>
Public participation	<p>ID providers can also raise awareness of the project and foster public ownership by having people participate in elements of the system design, such as crowd-sourcing contests to design ID system logos, songs, names, or card designs. To build trust and buy-in however, such activities must be done early in the project to be seen as authentic.</p>

Communications

Communication with the public and other stakeholders is fundamental for the success of an ID system. People need to *want* to register, *know how* to do so, and understand how the ID system will make their lives better or easier. Administrators will need to develop solid public information and education campaigns (IECs) during the initial program rollout, as well as ongoing communications strategies that adapt to emerging needs and issues. These communications efforts serve three primary functions:

- **Providing information about the process and requirements:** To participate in the ID system, the public needs to know: (1) *who* is eligible to enroll, (2) *when* and *where* to enroll, and (3) *how* to enroll, including which supporting documents or other evidence will be required. Without clear, consistent messaging regarding process and requirements, misinformation is likely to spread, creating barriers to participation.
- **Motivating people to participate:** Experience in multiple countries shows that people can feel very proud of their country when they participate in a national ID-type program. At the same time, people have often expressed ambivalence toward these systems when they see no value in them for their daily lives. Messaging, including clearly articulating the benefits of enrolling in the ID system—e.g., less paperwork, online transactions, links to social programs, ease of opening a bank account, national development, etc.—can help overcome these issues.
- **Alleviating fears and concerns.** In any country, certain individuals and groups (e.g., those with a history of marginalization or persecution) will fear having their data collected due to concerns about possible surveillance, discrimination, or data breaches. Through positive messaging—backed up by a privacy- and security-enhancing legal framework and design, along with positive registration experiences—IECs can help alleviate concerns and establish trust in the system.

IECs and ongoing communication strategies should take a multi-pronged approach using multiple media channels, formats, and styles to reach a broad audience that spans ages, social, economic, and linguistic groups (see Table 20).

Table 20. Communication format and channels

Media Format	Distribution Channels
Written communications	<ul style="list-style-type: none"> ▪ Print and online newspapers, magazines, blogs ▪ Social media (e.g., Facebook, Twitter) ▪ Agency websites ▪ Printed leaflets, posters
Videos	<ul style="list-style-type: none"> ▪ Television (commercials, special broadcasts, news shows) ▪ Social media (e.g., YouTube, Facebook), ▪ Agency websites
Songs, skits, and plays	<ul style="list-style-type: none"> ▪ Radio ▪ Television ▪ Public gatherings

Media Format	Distribution Channels
Public question and answers (Q&A) sessions by officials	<ul style="list-style-type: none"> Radio Television Public gatherings

The success of the initial years of an ID system—i.e., during mass registration and gradual adoption by service providers—depends on momentum, and IECs are crucial to this process. Specifically, they can showcase progress and good news stories, such as registration milestones, reduced waiting times, lower costs for opening a bank account etc. Using real stories from both regular people and celebrities can help boost the credibility of these messages (see Box 16 for examples).

Critically, system administrators must work to identify and publicly respond to people’s fears and concerns. Dismissing these concerns—e.g., by claiming that a database is not hackable or that the public has nothing to worry about—or working to discredit those who identify real vulnerabilities is only likely to *increase* mistrust in the system. Conversely, demonstrating an understanding and appreciation for these concerns through clear communication and visibly working to address these concerns will help strengthen the public’s confidence in the system.

Box 16. Examples of Information and education campaigns

In **Peru**, the national ID agency (RENIEC) and Coca Cola had a ‘Happy ID’ campaign, where people were encouraged to smile for their national ID card photo (see <https://www.mccannworldgroup.com/work/happy-id>). In addition, RENIEC maintains an active social media presence, including on [Facebook](#), [Twitter](#), and [YouTube](#).

In **Paraguay**, UNICEF leveraged a football match against Uruguay in its campaign for universal birth registration, with major TV and radio stations airing the first few minutes of the game without referring to the player’s names to highlight the importance of registration (see <https://www.youtube.com/watch?v=o0S-x>).

Japan’s “My Number” (a unique ID number system) has adopted a mascot to better brand the service (see <https://www.kojinbango-card.go.jp/mynumber/>).

Bangladesh created a theme song/video (in Bangla) for its new national ID card (<https://www.youtube.com/watch?v=GzK3F2yGCqg>).

ID4D has created a number of videos to showcase the impact that ID can have—available at <https://id4d.worldbank.org/videos>—including the Make Everyone Count video, a story of how Revenna’s ID got him his passport and the opportunity to attend the world cup, how a young refugee realizes her potential with the help of an ID, how digital IDs empower women cross border traders in East Africa, advancing financial inclusion through digital ID, and how near universal ID coverage in Peru leads to access to education.

Although communication is a critical element of ID system implementation, it is not sufficient to secure the buy-in and trust of the population. The process of public engagement should begin during the design of the project with meaningful public consultation that is perceived as genuine, rather than reactionary.

Grievance redress

ID systems require grievance redress mechanisms and infrastructure (e.g. a customer care department) through which individuals can file complaints about any aspect of the identity lifecycle. Potential grievances might include:

- Errors or misspellings in biographic information (e.g., name, address, etc.)
- Inability to enroll in the ID system (e.g., due to biometrics, lack of supporting documents, etc.)
- Frequent authentication failures (e.g., a high biometric FNMR)
- Mistreatment by registration agents
- Long waiting times for registration or authentication that create an undue burden
- Credentials are not available within the pre-specified time period (e.g., long wait time for ID card)
- Identity theft
- Lack of accessibility and accommodations at enrollment centers
- Unauthorized access or misuse of personal data

Grievance redress should be available through multiple channels, such as:

- In person (at registration points or other service centers)
- in writing
- By phone or SMS
- Online via websites, apps, email and social media

These channels should be supported by robust back-end systems to manage a call center and to keep track of grievances and the amount of time taken to resolve them. Service standards should be set and publicized to let people know how quickly their issue will be resolved and provide for measuring the effectiveness of the grievance redress mechanism. For this, significant budget needs to be set aside for properly staffing hotlines with enough operators and sufficient linguistic diversity, for procuring the necessary IT systems, etc.

Box 17. Examples of grievance redress mechanisms

To improve accountability to the beneficiaries of its in-kind and cash transfer programs, the **World Food Program (WFP)** uses call centers (phone lines) to field complaints and feedback and to conduct surveys. These centers are managed by professionally trained operators and include interactive voice response/recording (IVR) provides pre-recorded, interactive support for beneficiaries outside of working hours. In **Somalia**, for example, the number for the call center is printed on the cards used for beneficiary identification and displayed on posters in places served by WFP. The number can be called for free from any of the mobile networks. To follow-up on the calls, WFP relies on a team of 70-80 field monitors who can visit the site where the issue was reported and help put appropriate corrective actions in place (field monitors do this in addition to their broader monitoring responsibilities). WFP have emphasized that the real challenge is the follow-up, rather than encouraging reporting itself. They often also call the person reporting the issue back after some time to check whether it had adequately been addressed.

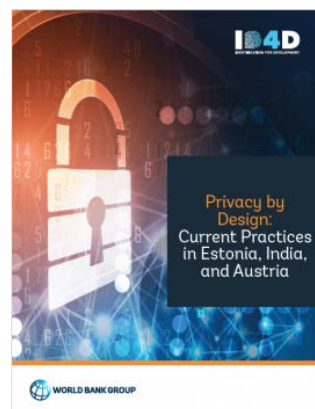
Source: <https://www.enonline.net/fex/56/accountabilitysomalialcluster> and conversations with World Bank Staff.

Complaints that are unresolved through standard grievance redress mechanisms may be handled by an independent supervisory authority, often with the ultimate recourse of judicial review, as set out in the legal and regulatory framework. Potential remedies include compensation if an individual has suffered material damage from violation of privacy rights and protections. Practitioners should prepare a grievance redress plan that sets standards and—in the event that multiple actors (e.g., enrollment agents, ID authority, etc.) are involved—clearly delineates roles and responsibilities.

PRIVACY & SECURITY

Maintaining user privacy and the security of systems that process—i.e., collect, store, use, and disseminate—personal data is a fundamental concern for ID systems as discussed in [Section II. Risks](#). In addition to adhering to international data protection and privacy principles in the development of the legal framework, privacy-enhancing technologies (PETs) and security measures should be built into every aspect of the ID system—that is, privacy assurance must become an organizational norm.

Achieving this goal can be done through adopting a “privacy-and-security-by-design” approach—first conceptualized by Anne Cavoukian as “Privacy-by-Design” or PbD ([Cavoukian 2011](#))—that adheres to the principles enumerated in Box 18.



Box 18. Foundational Principles of Privacy by Design (PbD)

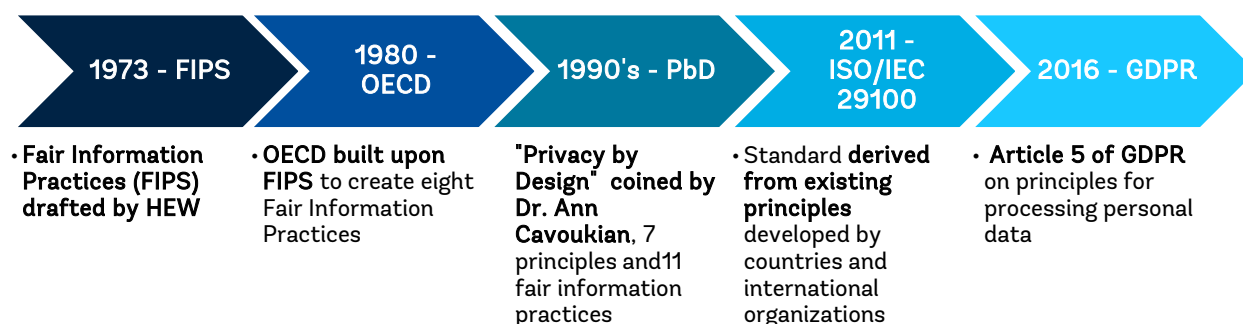
1. **Proactive not reactive; preventative not remedial:** The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred—it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.
2. **Privacy as the default:** We can all be certain of one thing—the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy—it is built into the system, by default.
3. **Privacy embedded into design:** Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.
4. **Full functionality; positive-sum, not zero-sum:** Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.
5. **End-to-end security; lifecycle protection:** Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved—strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.
6. **Visibility and transparency:** Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to both users and providers alike. Remember, trust but verify!

7. **Respect for user privacy:** Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric!

Source: *Cavoukian (2011)*.

As shown in Figure 12, the privacy-and-security-by-design approach embodies a number of global standards and principles on privacy and data protection that have been developed over the past few decades, including those discussed in *Section III. Legal Framework*.

Figure 12. Privacy frameworks for personal data



Source: *Privacy by Design: Current Practices in Estonia, India, and Austria*. For details on privacy frameworks, see *OECD (2013)*, *Cavoukian (2011)*, the *ISO/IEC 29100*, and *EU (2016)*.

Implementing a privacy-and-security-by-design approach requires complementary controls throughout the ID system lifecycle. This includes:

1. **Legal controls** for privacy and data protection, as well as information and cyber security;
2. **Management controls** for monitoring, oversight, and risk management;
3. **Operational controls** that promote security awareness, training, and detection; and
4. **Technology controls** that limit and protect the processing of personal data and ensure the physical and virtual security of systems that process this data (adapted from *ISO/IEC 29100*).

Each of these controls are complementary; on their own, each will be insufficient maximize the privacy and protection of personal information.

This section focuses on privacy- and security-enhancing technologies, design strategies, and operational controls—legal and management controls are discussed more thoroughly in *Section III. Legal Frameworks*. Privacy-enhancing technologies (sometimes called PETs) are a category of ICT measures, products, or services that protect privacy by eliminating or reducing PII or by preventing unnecessary or unauthorized processing of PII without losing the functionality of the system (*ISO/IEC 29100*).

As articulated in a recent report from the European Union Agency for Network and Information Security (ENISA) and summarized in Table 21, technology and operational controls can help protect personal data in multiple ways, including by *minimizing* data collection and processing, *hiding* personal data and their interrelationships, *separating* or distributing data processing, *aggregating* data to a level where it is not identifiable, *informing* people regarding data processing, giving *control*

over data processing, *enforcing* privacy policies, and *demonstrating compliance* with privacy legislation (Danezis et al. 2015).

Table 21. Examples of privacy and data protection enhancing technologies and operational controls

Strategy		Example solutions (not exhaustive)
Data-oriented	Minimize the collection and processing of personal data to limit the impact to privacy of the system	<ul style="list-style-type: none"> Collecting and sharing minimal data Anonymization and use of pseudonyms when data is processed
	Hide personal data and their interrelationships from plain view to achieve unlinkability and unobservability, minimizing potential abuse	<ul style="list-style-type: none"> Encrypt data when stored or in transit End-to-end encryption Key management/key obfuscation Anonymization and use of pseudonyms or tokenization for data processing “Zero semantics” or randomly generated ID numbers Attribute-based credentials (ABCs)
	Separate , compartmentalize, or distribute the processing of personal data whenever possible to achieve purpose limitation and avoid the ability to make complete profiles of individuals	<ul style="list-style-type: none"> Tokenization or pseudonimization by sector Logical and physical data separation (e.g., of biographic vs. biometrics) Federated or decentralized verification
	Aggregate personal data to the highest-level possible when processing to restrict the amount of personal data that remains	<ul style="list-style-type: none"> Anonymize data using k-anonymity, differential privacy and other techniques (e.g., aggregate data over time, reduce the granularity of location data, etc.)
Process-oriented	Inform individuals whenever their data is processed, for what purpose, and by which means	<ul style="list-style-type: none"> Transaction notifications Data breach notifications
	Give individuals tools to control the processing of their data and to implement data protection rights and improve the quality and accuracy of data	<ul style="list-style-type: none"> User-centric identity services Attribute-based credentials
	Enforce a privacy policy that complies with legal requirements	<ul style="list-style-type: none"> Role-based access control with two-factor authentication Remote access
	Demonstrate compliance with the privacy policy and applicable legal requirements	<ul style="list-style-type: none"> Tamper-proof logs Audits

Source: Framework adapted from Danezis et al. (2015) available at <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design> to fit the ID system context. This table is meant to be illustrative of common privacy-enhancing technologies and operational controls, but it is not exhaustive. For emerging solutions, users are also encouraged to consult the online, crowd-sourced catalog of privacy patterns currently being developed by UC Berkeley’s School of Information (see <https://privacypatterns.org/>).

The specific privacy- and security-enhancing operational and technical controls adopted by an ID system will depend on context and other design choices. Some important categories of these technologies and strategies are discussed in more detail below, including:

- Encryption
- Digital certificates and PKI
- Tokenization
- Platforms for personal access and control
- Tamper-proof logs
- Data center security
- Implementing a cybersecurity program

Encryption

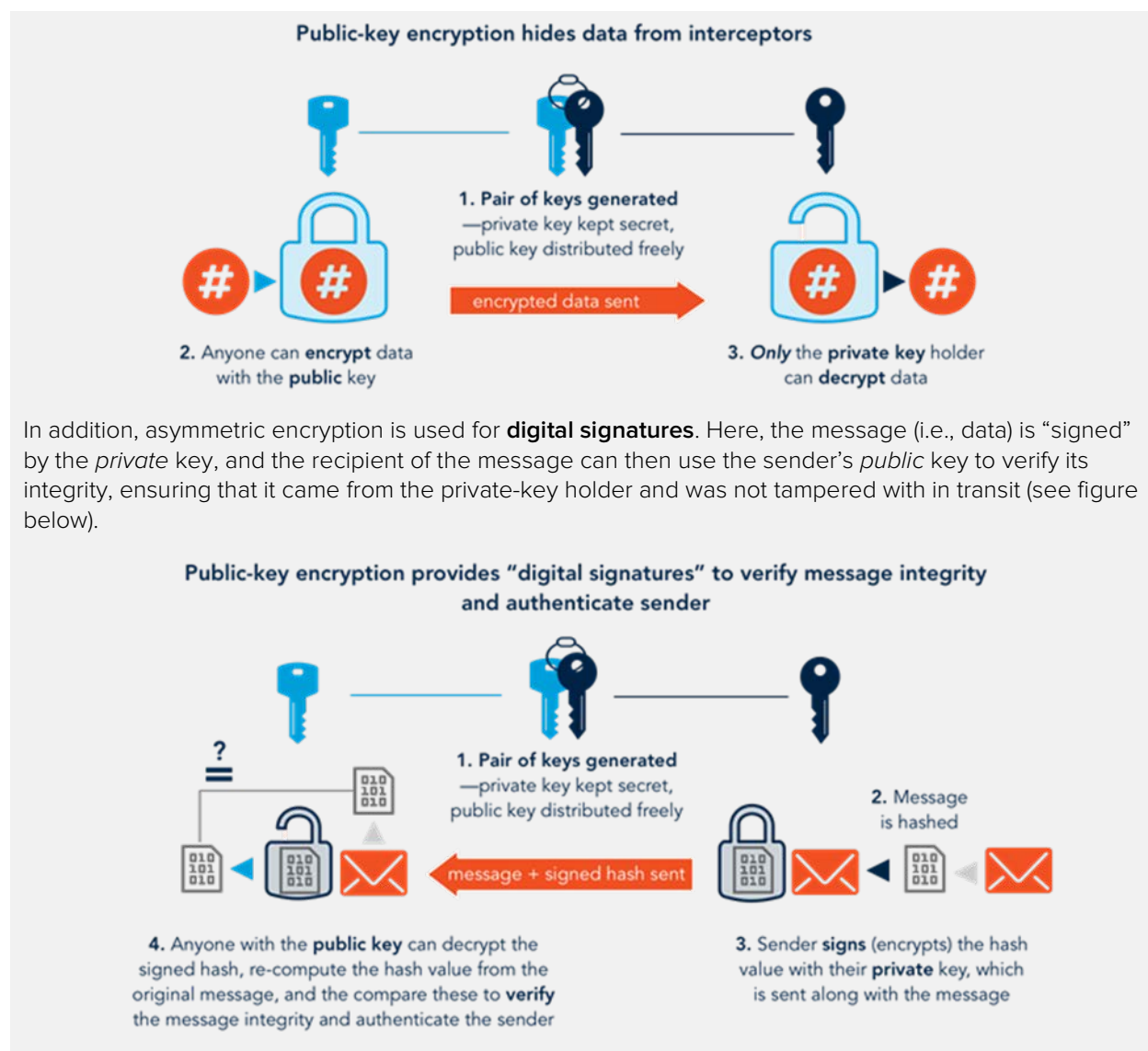
In any ID system, personal data is vulnerable to being accessed or intercepted and read by unauthorized actors during storage and when it is transferred. This includes when data is hosted in data centers or the cloud, and in particular during transactions that involve online authentication, verification, or exchange of identity data. For example, the majority of physical network links provide poor confidentiality and privacy for transmitted data, particularly where data must pass through the open internet. Although this may be convenient and efficient for users and administrators, it also leads to vulnerabilities that may expose personal data to a variety of attacks by eavesdroppers.

Box 19. Understanding public-key encryption and digital signatures

Encryption is the process of encoding information by inputting it—together with another parameter or “key”—into an encryption algorithm or “cipher.” There are two basic methods of encryption for securing data transmission:

- *Symmetric encryption:* A single key—a shared secret—is used to both encrypt (code) and decrypt (decode) information.
- *Asymmetric encryption (i.e., public-key encryption):* A pair of related keys are used; one to encrypt the data and the other to decrypt it.

In **public-key encryption**, a pair of keys are generated for an entity—a person, system, or device—and that entity holds the private key securely, while freely distributing the public key to other entities. Anyone with the public key can then use it to encrypt a message to send to the private-key holder, knowing that *only they will be able to open it* (see figure below).



Cryptographic methods are the most effective and commonly used tools for protecting data during storage and transactions. Specifically, both symmetric and asymmetric encryption (see Box 19) help protect the confidentiality and security of personal information by:

- **Hiding data:** Encrypted data are “locked” and cannot be read or understood by an interceptor or unauthorized user, except through a brute force attack that requires significant computing resources.
- **Sealing and authenticating data:** The use of asymmetric or public-key encryption allows senders to “digitally sign” a message or data so that the receiver can be sure that the sender is who they claim to be, and that the message was not tampered with during transit.

Given these functions, encryption plays multiple roles in ID systems, as shown in Table 22.

Table 22. Example requirements for data encryption in an identity system

Requirement	Description
Message Confidentiality	Encryption can prevent the interception and reading of messages in transit either at the user agent (e.g., a web browser) or in transit between trusted entities.
Message integrity	Ensuring the integrity of a message—i.e., that it was not altered during transmission—is often accomplished through the addition of a digital signature using public-key encryption.
Replay Protection	Encryption such as Secure Sockets Layer (SSL) can prevent “replay” attacks on authentication requests and responses. Other methods of replay protection include using public-key encryption to sign messages and setting a validity period for the message coupled with message request identifier tracking.
Transport Layer Protection	As a baseline all computer-to-computer communication should utilize the latest version of Transport Layer Security (TLS) as advised by national technical advisory bodies.
Eco-system Technical Trust	Authentication of entities in an ID federation based on cryptographic proof to ensure that only entities that are legitimate members are able to interoperate with the technical components of the federation scheme (e.g. identity providers, attribute providers, relying parties etc.).

Encryption technologies provide strong confidentiality protections but only for as long as the private keys used to ensure this protection remain secret. Therefore, key management is extremely important. These secret keys are a prime target for organized crime and other attackers as they effectively open access to the most valuable data held by organizations. It should also be noted that the methods of obtaining these keys are not restricted to technological means and often center on the identification of vulnerable targets for extortion, theft, coercion, and confidence tricks (e.g., phishing).

To minimize the possibility of data loss due to keys being compromised, steps should be taken to regularly rotate keys. This approach reduces the risk of data loss due to a key being compromised as any stolen keys will become useless at regular intervals and have a reduced scope for attack. For example, an automatic key rotation scheme such as Forward Secrecy ensures that a new set of keys are used for each communication session, and key are discarded once the session has ended. This means that sensitive data cannot be recovered and decrypted after the transmission has ended as the keys are no longer available. For this reason, it is recommended that no long-term secrets (keys) are used to protect the confidentiality of interactive end-to-end conversations in digital ID systems.

Digital certificates and PKI

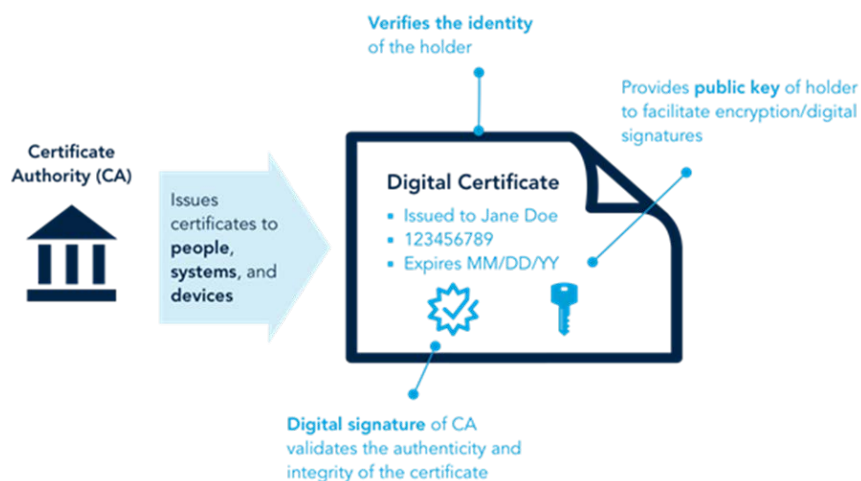
Digital certificates facilitate secure electronic communication and data exchange between people, systems, and devices online. They are issued by Certificate Authorities (CAs) and perform two primary functions:

- Verifying the identity of the sender/receiver of an electronic message
- Providing the means to encrypt/decrypt messages between sender and receiver (i.e., binding and entity to their public key)

There are three basic types of digital signature certificates:

- **Individual digital signature certificates (signing certificates):** These certificates are used to identify a person and include personal information. They can be used to sign electronic documents (i.e., to provide electronic signatures) and emails, and to implement access control mechanisms for sensitive or valuable information.
- **Server certificates:** These certificates identify a server (computer) and contain the host name or IP address. They are used for one- or two-layer SSL to ensure secure communication of data over a network.
- **Encryption certificates:** These certificates are used to encrypt a message using the public key of the recipient to ensure data confidentiality during transmission. Different signatures for encryption and digital signatures are available from different CAs. (adapted from *Government of India 2010*)

Figure 13. Digital certificates



A system—including policies, institutions, and technologies—that manages the distribution, authentication, and revocation of digital certificates is often referred to as public-key infrastructure (PKI). Because digital certificates are standard in data exchange and security protocols for digital ID systems (including the TLS encryption measures described above, as well as smartcard- and mobile-based authentication), a country's PKI landscape is a common building block for many ID systems.

For example, when a smartcard or SIM card that uses PKI for authentication and digital signatures is personalized, it is issued with a private key and digital certificate signed by a CA that attests to the authenticity of the credential and provides the public-key necessary for other devices (e.g., card readers, servers, etc.) to verify the authenticity and integrity of the card.

While it is possible for an ID provider to create its own digital certificates, it is often more practical and reliable to use a trusted third party as the CA and/or Root Certificate Authority. *Future versions*

of this Guide will include a deeper description of various options for setting up a PKI infrastructure, as well as alternatives.

Tokenization

Tokenization substitutes a sensitive identifier (e.g., a unique ID number or other PII) with a non-sensitive equivalent (i.e., a “token”) that has no extrinsic or exploitable meaning or value. These tokens are used in place of identifiers or PII to represent the user in a database or during transactions such as authentication. The mapping from the original data to a token uses methods—e.g., randomization or a hashing algorithm—that render tokens infeasible to reverse without access to the tokenization system.

Tokenization is not a new technology. In credit and debit card systems, for example, tokenization has long been used to replace data on the card (e.g. the primary account number or PAN), with a unique randomly generated token that can be used to represent the card data in transactions but does not reveal the original card data. This means that the number of systems with access to the original card data is dramatically reduced, and with it the risk of fraud should a system become compromised.

Tokenization can protect privacy by ensuring that only tokens, rather than a permanent identity number or other PII, are exposed or stored during a transaction. In addition—where the same person is represented by different tokens in different databases—tokenization can limit the propagation of a single identifier (e.g., a unique ID number). This can help limit the ability to correlate a person’s data across different databases, which can be a privacy risk and also increases the possibility of fraud.

The essential features of a token are: (1) it should be unique, and (2) service providers and other unauthorized entities cannot “reverse engineer” the original identity or PII from the token. There are two primary types of tokenization:

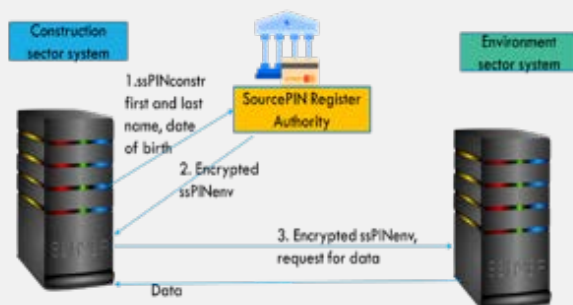
- **Front-end tokenization:** “Front-end” tokenization is the creation of a token *by the user* as part of an online service that can later be used in digital transactions in place of the original identifier value. This is the approach taken by Aadhaar to create a Virtual ID derived from **India’s** Aadhaar Number, as described in Box 21). The problem with front-end tokenization is that it is very user driven, requiring users to be digitally literate and technically capable of both understanding why they would need a token and how to create one online. This could easily lead to a digital divide with regard to privacy protection.
- **Back-end tokenization:** “Back-end” tokenization is when the identity provider (or token provider) tokenizes identifiers before they are shared with other systems, limiting the propagation of the original identifier and controlling the correlation of data. Back-end tokenization is done automatically by the system without user intervention, meaning that people do not need to do anything manually or understand why they would need to create tokens, eliminating any potential digital divide and protecting identifiers and PII at source. **Austria** is one example of this type of tokenization (see Box 20), and **India** has also implemented back-end tokenization of the Aadhaar number in addition to its Virtual ID (see Box 21).

Box 20. Austria's sector-specific identifiers

The data contained on **Austria's** virtual citizen card (CC, see Box 37) is called “Identity Link” and consists of full name, date of birth, cryptographic keys required for encryption and digital signatures, and the “SourcePIN”—a unique identifier created by strong encryption of the 12-digit unique ID (CRR) number. To ensure integrity and authenticity, the Identity Link data structure is digitally signed by the SourcePIN Register Authority at issuance. Access to SourcePIN and cryptographic keys on a CC is protected by PIN.

To safeguard user privacy, the eGovernment Act stipulates that different identifiers be used for each of the country's 26 public administration sections—e.g., tax, health, education, etc.— that a person accesses. A **sector-specific personal identifier (ssPIN)** is created from the SourcePIN using one-way derivation, a tokenization method through which a sector specific-pin is algorithmically computed from the SourcePIN.

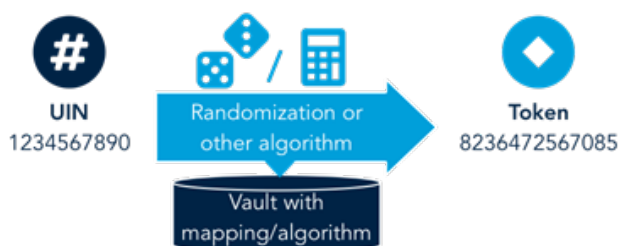
Unlike the SourcePIN, the ssPIN can be stored in administrative procedures. Public authorities can use the same ssPIN to retrieve a citizen's data stored within the same procedural sector, for example, if they need to view the citizen's records or use it to pre-fill forms. However, authorities do not have access to ssPINs from other sectors.

CROSS SECTOR DATA EXCHANGE - AUSTRIA

Administrative procedures often require authorities from different sectors work together. If authority “A” requires information about a person from authority “B” in another sector, authority “A” can request sector “B’s” identifier from the SourcePIN Register Authority by providing the identifier from their own sector, the person’s first and last name, and their date of birth. The SourcePIN Register Authority then sends the ssPIN from authority “B” to authority “A” in encrypted form; however, this can only be decrypted by authority “B”. In order to access the data, authority “A” then sends the encrypted ssPIN to authority “B,” which decrypts it and returns the requested data.

Source: *Privacy by Design: Current Practices in Estonia, India, and Austria.*

Although tokenization and encryption both obscure personal data, they do so in different ways, as shown in Figure 14. In general, tokenization is often simpler and cheaper to implement than encryption and has a lower impact on relying parties, as they do not need to decrypt data in order to use it. Tokens also have the advantage that, because they replace PII rather than hiding it like encryption, it is impossible to recover the original data in the case of a data breach.

Figure 14. Tokenization vs. encryption**Tokenization replaces personal data**

- The only way to recover PII is through the vault (makes exchange difficult)
- In case of a breach, token provides no meaningful information
- Preserves format and functionality of data (i.e., tokens can be searched, viewed, etc.)
- Only works with structured fields (e.g., numbers text fields, etc.)

Encryption hides personal data

- Anyone with the key can decrypt the data (makes exchange easy)
- In case of a breach, encryption can be broken through brute force attacks
- Does not preserve format or functionality of data (e.g., it must be decrypted to view, search)
- Can be used to protect files and documents, in addition to structured fields

At the same time, however, tokenization requires a means of mapping tokens to the actual identifier or PII data values (e.g. a token vault or algorithm)—with the most obvious options being through cryptography or reference tables. This can create issues with scalability, particularly where there is a need to access the actual user data in order to complete a transaction. For authentication this is not always the case, as there does not necessarily need to be disclosure of any personal data in order to prove that the individual is who they say they are. Implementations such as **GOV.UK Verify** (see Box 38) and **Aadhaar** (Box 21) are capable of managing the tokenization of identifiers at scale by avoiding the need to share data.

Box 21. India's Virtual ID and tokenization systems

In January 2018, the **Unique Identification Authority of India (UIDAI)** announced the introduction of two services for the Aadhaar unique ID system: (a) Virtual ID, and (b) UID token and limited KYC. Both features use tokenization to enhance the privacy and protection of Aadhaar holders' personal data.

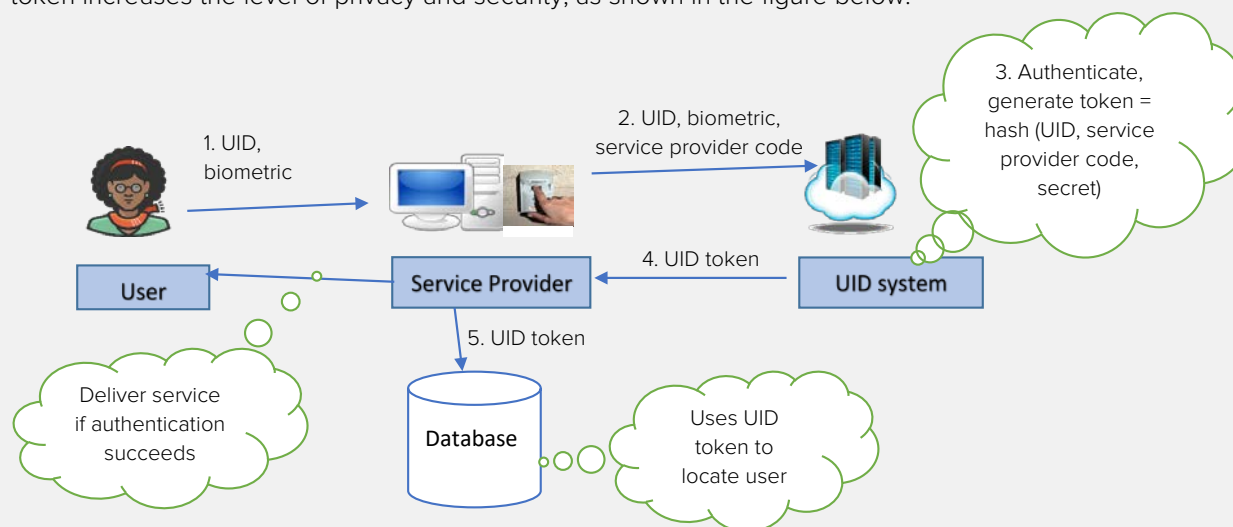
The **virtual ID** service involves **front-end** tokenization. It allows users to keep their unique, 12-digit Aadhaar number hidden from service providers by generating a random, 16-digit virtual ID number. This requires accessing the resident portal and authenticating themselves using an OTP sent on their registered mobile number. The virtual ID is mapped to the Aadhaar number by UIDAI. Once a person has generated a Virtual ID, they can provide that 16-digit number instead of their Aadhaar number for authentication; new Virtual ID numbers can be generated once every 24 hours.

A key privacy-enhancing aspect is that the Virtual ID is temporary and revocable. As a result, service providers cannot rely on it or use it for correlation across databases. Users can change their Virtual ID as needed, just as one would reset their computer password/PIN.

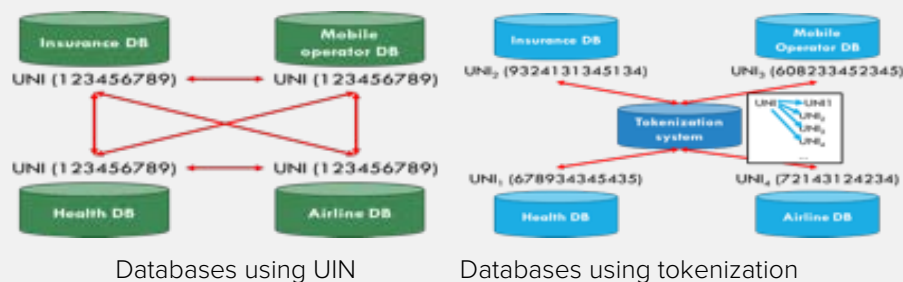
As a complement to the virtual ID, UIDAI also introduced **back-end tokenization** to address the storage of Aadhaar numbers in service provider databases. Now, when a user gives their Aadhaar number or Virtual ID to a service provider for authentication, the system uses a cryptographic hash function to generate a 72-character alphanumeric token *specific to that service-provider and Aadhaar number* which can be

stored in the service provider database. Because different agencies receive different tokens for the same person, this prevents the linkability of information across databases based on the Aadhaar number. Only UIDAI and the Aadhaar system knows the mapping between the Aadhaar number and the tokens provided to the service providers.

Subsequently, when the user authenticates with the service provider, the ID system again computes the token using the same hash function with Aadhaar number, service provider code and the secret message as inputs and generates the same UID token. The UID token would always be same for the given combination of Aadhaar number and service provider code. The combination of the Virtual ID and UID token increases the level of privacy and security, as shown in the figure below:



Certain service providers ("global AUAs") are allowed to store and use Aadhaar numbers and use the full eKYC API, which returns both the Aadhaar number and the token, along with the KYC data. Other service providers ("local AUAs") can only use the limited eKYC API using the token, and do not receive the Aadhaar number. This will limit the linkability of personal information across databases, as shown in the figure below.



Source: *Privacy by Design: Current Practices in Estonia, India, and Austria*. For more information on Virtual ID, tokenization, and limited eKYC in India, see https://uidai.gov.in/images/resource/UIDAI_Circular_11012018.pdf.

Platforms for personal oversight

A central tenant of the privacy-and-security-by design approach and international principles for privacy and data protection is that individuals have the right to access and correct their data, and to monitor how it is being used by governments and third parties (and to hold these actors accountable for misuse). In addition, these standards require general openness and transparency

regarding the policies and practices related to personal data management, which should be readily available and accessible to individuals.

One way to implement personal oversight of data use is to create a platform or portal (e.g., accessible through the internet, smartphone apps, USSD, and call centers) where individuals can log-in and view their personal information and records of who has accessed their data, when, and why. As shown in Box 22, this is one of the strategies that **Estonia** uses, in combination with other features—such as tamper-proof logs—to protect privacy and ensure compliance with data protection laws. **India** also has a portal where residents can view a record of authentications using their Aadhaar number. Such portals can be an important part of empowering individuals to have control over their data.

At the same time, platforms that require internet access may be exclusionary for individuals in low-connectivity areas or those with low levels of digital literacy. Thus, practitioners should ensure that people have access to other procedures (e.g., at physical offices) and grievance redress mechanisms to view and correct errors in their data and oversee who has used it, and for what purpose. In **India**, for example, notification via email every time an Aadhaar number is used for authentication addresses some of these exclusion concerns.

Box 22. Estonia's citizen portal

Estonia's citizen portal (eesti.ee) provides residents with a number of tools to oversee and control their data. First, it allows users to **see who has access their data** via the Personal Data Usage Monitor that logs all transactions containing personal data (see Box 23). A resident can check these logs for any unauthorized usage of their data, and then contest any unsanctioned access.

Second, it gives users the **ability to control which data is shared with whom**. With health services, for example, patients can view all their electronic health records (EHRs) through the Estonian eHealth Patient Portal, by using their digital ID to authenticate their identity. By default, medical specialists can access data, but any patient can choose to deny access to care providers, including their general practitioner or family physician. Other users, such as pharmacists and insurance agents, can get access to a patient's medical records, but only with the patient's explicit knowledge and consent. All data access requests within the system are recorded, and patients can access this record on request (see <https://e-estonia.com/solutions/healthcare/e-health-record/>).

These technical oversight mechanisms are complemented by Estonian **data protection laws**, which stipulate heavy penalties for unauthorized access to data. There have been reported cases of punishment of law enforcement officer for unauthorized data access for personal gains. A dedicated data protection authority handles grievances and complaints.

Source: *Privacy by Design: Current Practices in Estonia, India, and Austria*.

Tamper-proof logs

Ensuring that personal data are only accessed by authorized users—and for authorized purposes—requires some method of tracking transactions and who has accessed the data and when. Automatic, tamper-proof logging of transactions involving identity data is a best-practice method for enabling both institutional and personal oversight of how these data are being used.

Any logs or audit data collected must comply with privacy and data protection requirements for the ID system in question. At a minimum, logs should be:

- protected from unauthorized access (and have that use monitored);
- protected from unauthorized copying or exfiltration; and
- devoid of personal data.

In **India** and **Estonia**, for example, logs are digitally signed to detect tampering. In addition, chaining digitally signed logs in **Estonia** makes it difficult to change their history (see Box 23). Using emerging technologies such as blockchain may also have the potential to increase the security of these logs by making them immutable, even to the agencies that maintain them.

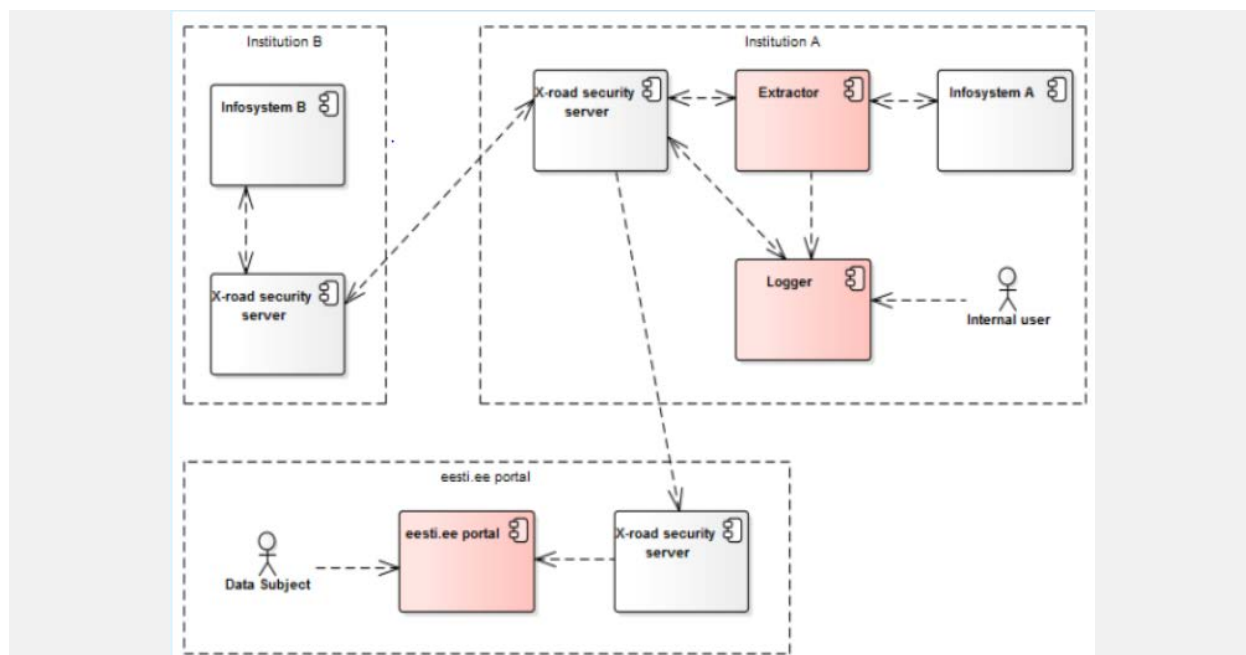
In addition to facilitating audits of data use, logs are of vital importance in instances of fraud or security breaches, as they will form the basis of investigations or reviews of system activity and data access. The tamper-proof nature of the logs is also crucial, as attackers who gain access to the underlying IT systems may attempt to alter or delete this information. It is therefore important to put in place systems and technologies that minimize the risk of such attack and ensure the integrity and security of audit logs, such as:

- Ensuring that logs from application servers are removed as soon as possible and sent to a central log management system
- If possible, sending log data directly to a centralized log management system
- Making sure that log files and log transactions are encrypted in transit and at rest
- Ensuring that the centralized log management system has sufficient access control and authentication as well as access audit logging
- Applying role-based access to log file systems to ensure that only authorized personnel may perform actions such as deleting log files
- Analyzing log file activity to identify gaps in logging or patterns of corruption which may highlight suspicious activity

Box 23. Tamper-proof logs in Estonia

Estonia's Personal Data Usage Monitor (open source software available at <https://github.com/e-gov/AJ/blob/master/preliminary/Overview.md>) filters and logs transactions containing personal data. It is used at the exit points of information systems from where the data flows to other systems. This independent software can capture transactions containing personal data based on rules defined to identify personal data in data traffic flowing out of a system and log them with timestamp and digital signature.

As shown in the figure below, an “extractor” component creates a record each time a resident’s data is accessed, which contains metadata about usage. A “logger” component logs this event in time-stamped, digitally signed tamper proof logs. The system/database owners cannot choose which transactions to log or hide/delete transactions.



These logs are then accessible to the users via the **citizen portal** (eesti.ee, see Box 22), offering a comprehensive view of how personal data has been used by the government (and the opportunity to contest in the case of misuse). Internal system users also check the logs to monitor the activity and flag anomalous behavior for preventive and corrective measures.

Source: *Privacy by Design: Current Practices in Estonia, India, and Austria*.

Operational security controls

Operational controls that maintain the security and integrity of ID system facilities, data centers, and equipment are paramount to protecting personal data. Data breaches can come from multiple internal and external sources, including employees who fail to follow security procedures, hackers who gain access to inadequately-protected databases, and thieves who steal unsecured portable devices. In order to reduce these threats, ID system operators should employ state-of-the-art measures to reasonably prevent, detect, mitigate and respond to third party attacks, unauthorized access, and malicious or fraudulent use.

There are many international standards aimed improving data center management, security, and access control, including *ISO/IEC 27001* (information security management systems), *ISO/IEC 22301* (business continuity management), and *ISO/IEC 55000* (asset management). In particular, ISO/IEC 27001 focuses on developing an information security management system (ISMS) that provides a systematic approach to securing sensitive information by applying a risk management process to people, processes, and IT systems.

Many organizations choose to gain ISO/IEC 27001 accreditation as proof of compliance; however, it may be more useful to take the standard as a baseline for information security management, alongside any other relevant standards such as the Payment Card Industry Data Security Standard ([PCI DSS](https://www.pcisecuritystandards.org/)).

Operational controls must address both physical and virtual security. Virtual protections include:

- Access control (Identity Access Management on all work stations);
- Firewalls; and
- Intrusion Detection Systems (IDS).

For physical assets, any security management strategy should also seek to implement measures that address the following concerns and questions, further described in Table 23:

- **Building and asset security.** Visitors to any physical data centers, card-personalization centers, or other ID facilities and assets should be required to gain access through a rigorous building security process and, once admitted, be restricted to specific areas, assets, or systems based on their role and purpose.
- **Policies and processes.** Policies and processes related to access control are only effective if they well understood and regularly practiced by staff. Security training should be provided to all staff on an ongoing basis.
- **Staff.** Security is a concern for everyone, particularly staff within ID facilities. Staff should be knowledgeable, vigilant and able to understand organizational objectives with regards to security.
- **Contractors.** Where contractors or suppliers (e.g., engineers, cleaning staff, etc.) are regularly working within ID facilities, their credentials should be checked to ensure that the risk of a breach is mitigated.

Even with adequate safeguards or oversight, it is impossible to make a digital system completely immune from a breach. In the event that breaches do occur, breach notification laws generally require data controllers to inform individuals and/or authorities that a breach has occurred (see Table 23).

Table 23. High-level checklist for the physical security of ID systems

Key Questions	
Building & asset security	<ul style="list-style-type: none"> <input type="checkbox"/> Are there a wide range of access controls in place including? <input type="checkbox"/> Are access controls configured to utilize multi-factor authentication? <input type="checkbox"/> Are data center areas housing server infrastructure windowless and with a minimum safe number of entry points? <input type="checkbox"/> Are the server racks and cages in the data center unmarked and anonymous? <input type="checkbox"/> Are server racks and cages locked with access strictly controlled and monitored? <input type="checkbox"/> Is CCTV monitoring used in sensitive areas of the data center 24x7, and if so is this monitoring carried out by an onsite network operations center (NOC)? <input type="checkbox"/> Do security staff have the capability to protect themselves in the event of an attack on the data center and react accordingly? <input type="checkbox"/> Is there the capability to directly alert the police in the case of unauthorized access?

Key Questions	
Policies & Processes	<ul style="list-style-type: none"> <input type="checkbox"/> Are there processes in place to grant and remove access to facilities and individual resources (e.g. server racks) for both internal and external personnel? <input type="checkbox"/> Are user commands such as logins, file opens, downloads and file saves monitored for aberrations in pattern? Are “events” transferred to analysts for real-time assessment and response? <input type="checkbox"/> Is a record kept of all access to the data center and retained securely for a specified period of time? <input type="checkbox"/> Are data center staff, visitors and contactors only granted access to sensitive areas, racks and cages based on stated and verified need? <input type="checkbox"/> Are all visitors to the data center accompanied by staff unless otherwise authorized? <input type="checkbox"/> Is it easy to visually identify staff, visitors, and contractors based on the type of ID badge that they wear in the data center? <input type="checkbox"/> Are ID badges assigned and managed under a suitable policy and operated by a capable authority (e.g. a NOC)? <input type="checkbox"/> Is the installation, removal or maintenance of equipment in the data center controlled and monitored? <input type="checkbox"/> Do staff receive regular training on security procedures and requirements?
Staff	<ul style="list-style-type: none"> <input type="checkbox"/> Are there staff on site who can answer a full range of auditors’ questions and produce certifications, should they be required? <input type="checkbox"/> Are they able to share general advice around data center security and compliance? <input type="checkbox"/> Are senior security personnel based at the data center itself rather than a remote site? <input type="checkbox"/> Are data center staff required to undergo background checks where necessary? <input type="checkbox"/> Are they sensitive to the ID system’s confidentiality requirements (e.g. not disclosing personal information)?
Contractors	<ul style="list-style-type: none"> <input type="checkbox"/> Where suppliers are allowed to enter the data center unaccompanied, will ID holders be informed about which suppliers have access? <input type="checkbox"/> Are ID holders able to access basic information on contractor agreements, authorization levels, and any policies and processes in place to control and monitor contractor activity within the data center? <input type="checkbox"/> Are contractors accredited or vetted to any required standards?

Implementing a cybersecurity program

It is recommended that practitioners implement a cybersecurity program to build the capacity of the ID authority to protect its assets and the capacity of the central cybersecurity agency to perform a supportive and enabling role. Since government budgets may not be enough to fund high-end security arrangements for every information asset, this involves the identification and allocation of risk profiles and their associated tolerance levels to guide the level of safeguarding of each ID system asset. A formal recognition of the ID system as a critical national information

infrastructure (CNII) may be adopted so that high-end security arrangements and respective budgets can be allocated.

A cybersecurity program for the ID system may also include the following implementation activities, among others:

1. **A legal framework on cybersecurity.** Enactment of good practice Cybercrime and Cybersecurity legislation (discussed earlier in [Section III. Legal Frameworks](#)).
2. **Sectorial cybersecurity strategy for the ID system.** To supplement a national-level cybersecurity strategy document, a sectorial cybersecurity strategy focused on the ID system may be considered.
3. **Cybersecurity foundations.** To strengthen the safeguarding of private data and ID systems, activities to provide the necessary cybersecurity foundations are recommended. These include (a) a cybersecurity architecture to work in complementarity with the technical design of the system ex ante and by design; (b) a cybersecurity work and action plan with clear delineations of responsibilities and roles to be created and implemented, with an annual evaluation and revisions as needed; (c) a set of compliance standards for cybersecurity across sectors; (d) a trust and transparency framework; (e) best practice ISO certification of the primary provider of cybersecurity for the ID authority.
4. **Intelligence monitoring, detection and analysis.** An important first step for cybersecurity is collecting intelligence on potential threats and risks. Recommended activities for consideration are: (a) a risk analysis; (b) systems and software to enable capable threat intelligence for the ID ecosystem; (c) an ID system security operations center (ID-SOC) team to undertake threat intelligence and monitor the critical information infrastructure assets of the sector; (d) tools to detect human and physical vulnerabilities; (e) fraud detection tools; (f) recruitment of a certified chief information security officer (CISO) and team for the ID authority; (f) capacity building and ongoing skills development for the ID authority and selected partners, with a strategy to overcome human resources turnover challenges.
5. **Prevention.** Once hackers have successfully penetrated a system, mitigation and recovery can become costly endeavors in terms of time, effort and budget. A key element of a cybersecurity program is therefore prevention. Recommended activities are: (a) technical solutions for the safe transfer and interoperability of data through encryption and standards; (b) reinforcing the public key infrastructure (PKI) for identification; (c) regular cyber risk assessments undertaken of the ID authority and its partners; (d) regular audits of the ID authority's infrastructure and processes by external vendors; (e) regular penetration tests by certified ethical hackers and by the national CERT to identify vulnerabilities.
6. **Enforcement.** If the country or ID authority have a hub-and-spokes model for its cybersecurity processes, one or both of their roles may be to enforce the cybersecurity of partners. To achieve this, it is recommended to consider: (a) an evaluation and audit framework for partners; (b) regular cybersecurity audits of partners spanning government agencies and private sector licensed partners to ensure compliance; (c) certification of partners' hardware and software; (d) cybersecurity requirements for the licensing of partners.

7. **Reporting, Response and Mitigation.** Depending on the institutional and governance structure set out by the country's national cybersecurity strategy or policy, the national-level CERT could be supplemented by a CERT for the ID sector. Where needed, this could include: (a) establishment of an ID-CERT to link to the national CERT and provide the necessary sectorial support; (b) institutional, governance and technical mechanisms and procedures for agencies to report incidents to the ID-CERT; (c) response and mitigation tools, mechanisms and procedures by the ID-CERT; (d) hardware and software support for the ID-CERT team; (e) capacity building and ongoing skills development for this team, with a strategy to overcome turnover challenges. Such arrangements may be more applicable in larger countries, whereas in smaller economies, the national CERT would take on these roles.
8. **Recovery.** In the event of a breach, a crucial element of a Cybersecurity program is to recover and regain regular operating levels as quickly as possible. Recommended activities to achieve this include; (a) defining a business continuity plan that takes into consideration the business operation for the ID ecosystem; (b) exercising and testing of the business continuity plan; (c) defining a disaster recovery plan that takes into consideration the infrastructure operation for the ID system, including redundancy; and (d) related capacity building.
9. **Capacity building and skills development.** To provide the ID authority and its partners with the skills required to deploy Cybersecurity standards as required, recommended activities are the needed skills development for Cybersecurity managers and technical staff: (a) technical training for officials and selected partners; (b) regularly reviewed skills gap analyses and capacity building plans; (c) tailored awareness raising for management and budget deciders; (e) capacity building for the ID-CERT, ID-SOC teams and the business continuity/disaster recovery efforts; (f) a strategy for overcoming turnover challenges of staff moving to more lucrative employment after they have been trained.

ADMINISTRATION

The administration of an ID system—including the organizations, staff, and procedures involved in its management, operations, and oversight—is critical to ensuring that the system is trusted and sustainable. For example, common success factors for ID systems include:

- ID authorities with the technical capacity and human, political, and financial resources to effectively manage the ID system
- A high-level of cooperation and input into the ID system from diverse stakeholders that is built into the governance of the ID project (e.g., through an advisory board or steering committee, civil society consultations, inputs from international experts, etc.)
- Independent bodies that are legally empowered and have the capacity to oversee ID-related activities and hold responsible parties accountable

Key decisions for the administration of an ID system include:

- Which entity will be the ID authority with ultimate responsibility for the system and how will it be governed?
- What roles will the ID authority and other stakeholders play throughout the identity lifecycle?
- What business model will be adopted?
- How will frontline services (e.g., registration, data updates, credential replacement, and grievance redress) be delivered at the local level? (*coming soon!*)
- What change management processes and staff training will be in place? (*coming soon!*)

ID authority and governance structure

For new ID systems, choosing the institutional home and governance structure of the ID authority is a first-order decision. ID authorities are specialized entities responsible for implementing and/or overseeing the collection, verification, storage, and sharing of personal identity data, credential issuance, and the verification and authentication of identity data. They are also typically responsible for public engagement and grievance redress.

In order for an ID system to succeed, this entity must be empowered by law and political will and should demonstrate the capacity to serve as a champion of identity, a convener of multiple stakeholders, and an effective implementor and/or overseer. Because of the sensitive nature of its responsibilities, the ID authority should spend considerable time and resources to build the confidence of the public in its capabilities. The responsibility of the ID authority should be clearly defined and should be balanced and managed with the assistance of other government agencies, the private sector, and broader identity stakeholders. Strong provisions for the effective governance of the ID authority must be put in place.

As shown in Table 24 and Table 25, **there are multiple potential institutional arrangements for an ID authority:**

- It can be an autonomous entity governed by a board representing stakeholders, or with direct cabinet- or executive-level reporting
- Alternatively, it may be an agency or directorate within an existing ministry or department, also potential governed with a board
- It may be responsible for ID only, or for ID and civil registration

The adoption of one model over another is typically a function of the historical development of these systems, as well as institutional capacity and political considerations. In many countries, legacy identification and civil registration systems have traditionally been located in Ministries of Interior, Home Affairs, Justice, Local Government, and local government has typically been involved in frontline service delivery. In contrast, autonomous ID providers—e.g., India, Peru, Nigeria, etc.—are a relatively new phenomenon, and have been adopted over the past few decades to implement new ID systems in countries where legacy systems were weak or non-existent. The emergence of autonomous ID authorities also reflects a fundamental paradigm shift from ID systems being used as systems to control or monitor the population to systems that enable services and inclusion for the entire government or economy.

Table 24. Institutional arrangements for ID authority

	Agency or Directorate within Ministry	Semi- or Fully-Autonomous Agency
Same as central CR or NPR	Botswana, Chile, Ecuador, Indonesia, Jordan, Namibia, Rwanda, Thailand (most have separate units for ID/CR within agency, and local governments)	Peru, Philippines (<i>planned</i> PhilSys system)
Different than CR or NPR	Kenya, Morocco, Spain	India, Ghana, Nigeria

Although unifying the administration of ID and CR is not a requirement for implementing an ID system, it can create a number of efficiencies. Ensuring legal identity from birth, for example, requires strong linkages between ID and CR, which may be operationally easier if both are the responsibility of one agency. At the same time, however, linking ID and CR systems can also be accomplished by separate departments or agencies who operate under a strong framework of cooperation and coordination, as well as with appropriate mandates under relevant laws and regulations and technical interoperability.

As the more “modern” institutional arrangement for managing ID systems, **autonomous authorities have a number of advantages:**

- Establishing a new ID agency can be a “clean break” with the past and help interrupt cycles of inefficiency or legacies from unsuccessful previous projects.
- Autonomous agencies can potentially be seen by other ministries as “neutral” and a service provider, and thus in a position to avoid legacy or institutional mandate conflicts between existing ministries.
- In certain contexts, autonomous, independent agencies may be more trusted by the population to manage personal data than ministries or departments linked to national security and law enforcement/
- Autonomous authorities that manage their own staffing and resources may be better able to implement meritocratic hiring practices that attract top talent and ensure sufficient technical capacity.
- Fiscal autonomy gives authorities the ability to raise their own revenue (e.g., through fees for services), potentially making them self-sustaining.
- Particularly where they have some amount of fiscal independence, autonomous authorities may be better able to maintain independence during political transitions (i.e., elections).

At the same time, however, creating a new authority with sufficient power and capacity may be difficult in certain contexts.

In a data-centric world, the role of any authority that deals with identity will grow in importance over time, as more data accumulates and the dependency on system increases. **To maintain checks and balances over such organizations, a robust multi-layer institutional governance structure is needed.**

As summarized in Table 25, ID authorities that are agencies or directorates within an existing ministry will report to that ministry, while there are several different potential governance models for autonomous agencies, including reporting directly to the executive branch (e.g., a presidential office or cabinet) or to a board of directors.

Table 25. Governance models for ID providers

Organizational Type	Examples
Autonomous, with direct Cabinet- or Executive-level reporting	<ul style="list-style-type: none"> ▪ India: Initially, the Unique Identification Authority of India (UIDAI) was set up as an organization attached to the Planning Commission of India, reporting to a Chairman who had the status of a cabinet minister. Following the passage of the Aadhaar Act in 2016, UIDAI became a statutory authority responsible for implementation of the Act, under the Ministry of Electronics and Information Technology. ▪ Ghana: The National Identification Authority of Ghana was set up as an organization within the Office of the President.
Autonomous, governed by a board representing stakeholders	<ul style="list-style-type: none"> ▪ Nigeria: The National identity Management Commission (NIMC) is governed by a board of 18 individuals representing different government agencies and stakeholders. ▪ Philippines: The Philippine Statistics Authority (PSA) is governed by a board of representatives of 28 Government departments and commissions and one representative of the private sector, chaired by the Secretary of Socio-economic Planning. The Philippine Identification System (PhilSys) Policy and Coordination Council, comprising a subset of these departments but also chaired by the Secretary of Socio-Economic Planning, will oversee the implementation of the PhilSys.
Agency or directorate within an existing Ministry	<ul style="list-style-type: none"> ▪ Thailand: The Bureau of Registration Administration (BORA) under the Department of Provincial Administration (DOPA) of the Ministry of Interior. ▪ Argentina: The <i>Registro Nacional de las Personas</i> (RENAPER) is a directorate under the Ministry of Interior and Transportation.

Source: Adapted from the *Digital Identity Toolkit*

In addition to direct oversight by a ministry, the Executive, or a board of directors, a variety of other structures are needed to strengthen the governance of ID systems. One such structure for an could consist of multiple specialized committees such as the following:

- **Executive/Board:** This is the highest-level governance body, with representation at the executive level from across government, and often also civil society and the private sector. It would typically be responsible for setting strategies, policies and objectives and providing strategic oversight.

- **Technical steering Committee:** This body, reflecting the Board but at the technical-level, translates the strategies, policies and objectives set by the Board into operational plans. It oversees the work of various subcommittees in specific domains, such as:
 - **Technology Sub-Committee:** This body provides direction regarding the adoption and use of technologies, including technical standards, policies (e.g. open source software or cloud data storage) and design choices.
 - **Use Cases and Authentication Sub-Committee:** This body provides direction regarding the services provided to relying parties, including authentication and verification services. It may also be responsible for reviewing applications for access to the ID system.
 - **Legal Sub-Committee:** This body provides direction regarding the development and review of relevant laws and regulations.
 - **Public Engagement Sub-Committee:** This body provides direction regarding consultations and public information and awareness campaigns.
 - **Financial Management Sub-Committee:** Oversees and manages planned capital and operational funding usage. Monitors the financial performance metrics for the ID authority.
 - **Risk and Compliance Sub-Committee:** Ensures that risks (e.g., to privacy, security, and exclusion) are identified, assessed, and mitigated in a reasonable and coherent manner for the whole ID system.
- **Independent Auditor and Oversight Body:** An independent supervisory or regulatory authority is a critical component of the ID authority's institutional governance. It is typically put in place to ensure the compliance of the ID authority with its mission and laws related to data protection and privacy. It is the body that enhances the trust in the organization and its independence has to be a high priority for the government.

In addition to long-term governance arrangements, some countries consider **temporary institutional arrangements** for the start-up phase of their ID systems. This can help ensure a rapid launch and efficient project management in the short term while allowing enough time to set up more robust organizational structures in the long term (see Box 24).

Box 24. Temporary institutional arrangements for the startup phase of an ID system

India (2009) — attached office

The Unique Identification Authority of India (UIDAI), responsible for Aadhaar, was established by notification in January 2009 as an attached office to the then Planning Commission of India. Following the appointment of UIDAI's Chairman in July (at the rank of Minister, sitting in Cabinet meetings when Aadhaar was discussed), the Prime Minister's Council on UIDAI was set up to oversee the development of UIDAI's overall strategy and to ensure the coordination across Government.

In addition, the government set up a Cabinet Committee on UIDAI related issues in October 2009, chaired by the Prime Minister with 12 Ministers as additional members. The Committee oversaw UIDAI's

organization as well as its plans, policies and implementation progress for the rollout of the Aadhaar program, including overseeing two technical committees on biographic and biometric standards.

Following the passage of the Aadhaar Act in 2016, UIDAI became a statutory authority responsible for implementation of the Act, under the Ministry of Electronics and Information Technology. By 2016, over a billion people had been registered and issued an Aadhaar number.





Uganda (2013) – temporary project

Uganda's national ID system was launched in November 2013 as the National Security Information System (NSIS) project. The project approach was adopted to expedite the mass registration of citizens in time for the February 2016 elections, including by leveraging expertise of a range of agencies. Provisions for the registration of citizens in the Uganda Citizenship and Immigration Control Act provided a legal basis for the project. While the project was led by the Ministry of Internal Affairs, which has responsibility for implementing the Act, it was formally implemented jointly by the following agencies:

- Directorate of Citizenship and Immigration Control – validated citizenship of registrants
- National Information Technology Authority – provided technology compliance assurance, quality assurance leadership and technical support
- Uganda Bureau of Statistics – provided expertise from managing census operations
- Electoral Commission – ensured compliance with electoral laws
- Uganda Registration Services Bureau (URSB) – as the agency responsible for civil registration
- Uganda People's Defense Force and Uganda Police Force – providing human resources for the mass registration

The mass registration was completed by August 2014. Following passage of the Registration of Persons Act in March 2015, the National Identification and Registration Authority (NIRA) was established as a semi-autonomous agency to be responsible for the national ID system and civil registration, assuming the latter responsibility from the URSB.

Figure 15. Key considerations for the institutional home and governance of the ID authority

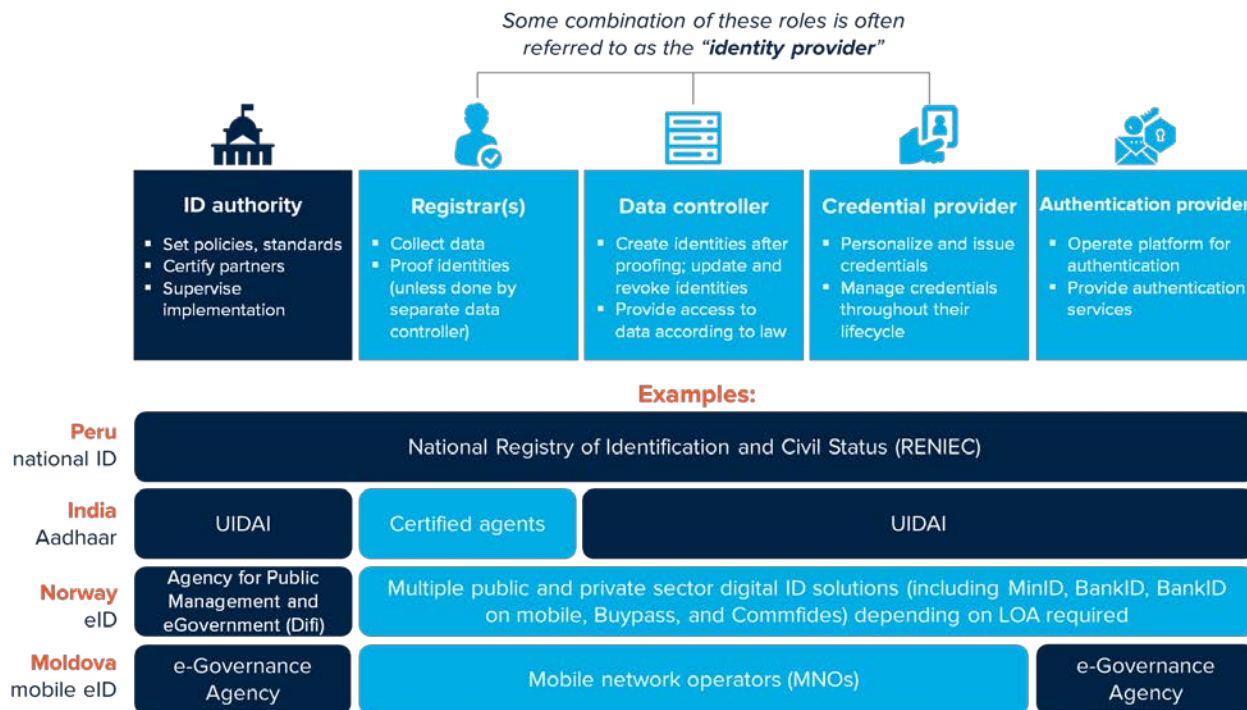
 Inclusion	 Reliability	 Data Protection	 Sustainability
Whether the same as the CR agency or not, coordination with the CR is crucial for ensuring inclusive and streamlined identity services from birth to death.	The ID authority must have sufficient technical expertise to implement and/or oversee a trusted ID system and to deliver services at the local level.	As custodians of personal data, the capacity of the ID authority and its oversight bodies to protect this data is paramount to the overall success of the system.	The ID authority must have sufficient resources with which to implement their mandate, whether from state budget or own revenue.

Roles and responsibilities

Although the ID authority has primary accountability for the implementation of the ID system, their role throughout the identity lifecycle may be lean or robust. Beyond setting overall standards and policies and engaging with the public, **the ID authority may also fill one or more of the following roles throughout the identity lifecycle:** (1) collecting and proofing identity data, (2) managing

identities and data, (3) issuing, replacing, and revoking credentials, and (4) providing identity authentication and verification services (see Figure 16).

Figure 16. Example institutional roles within an ID system







Source: Adapted from the *Digital Identity Toolkit*, with information on Norway from <http://eid.difi.no/en/how-register-new-user-id-porten>.

The division of roles has important implications for the overall functioning of the ID system as well as costs and data protection and privacy. In some cases—e.g., **Peru**—the ID authority fulfills all of these roles. In other cases, these roles may be assigned or adopted by different agencies, implemented in partnership with the private sector, or outsourced entirely. Vertical integration of ID-related activities has some benefits, including clear lines of authority and accountability for the ID system. At the same time, partnerships and/or the outsourcing of some functions may allow the ID authority to lower its initial investment costs and keep a relatively smaller footprint. This has been the route taken for some countries—e.g., the **UK, Sweden, Norway, Denmark, and Moldova**—creating digital authentication layers and services to facilitate log-in for e-services.

From a privacy perspective, it may also be advantageous to divide the responsibilities of the ID system between multiple actors, such as separating the roles of authentication provider and authorization provider from identity provision. This “**separation of duties**” limits the power of any single entity, potentially reducing the risk associated with a single “rogue” administrator or agency. In addition to separating roles within the identity lifecycle, it implementing the principle of “**least privilege**”—which ensures that any administrator only has the powers necessary to perform their delegated function, and no more—will also help protect personal data from misuse (see the *IDEEA* framework for more).

Another argument for devolving the authentication services is that it may encourage innovation. Levels of assurance and the nature of the service will differ by use case, and providers of authentication services may be able to offer the appropriate technology better than a centralized agency. They may also be in a better position to make the requisite infrastructural investments than a government entity (e.g., the banking sector).

Figure 17. Key considerations for roles and responsibilities

 Reliability	 Data Protection	 Sustainability	 Responsiveness
All entities involved in the ID lifecycle must be capable and trusted to manage core processes.	Separation of duties across agencies may help limit power and provide checks and balances for the ID system.	Well-implemented partnerships may reduce upfront costs and footprint of the ID authority.	Lines of accountability may be clearer in cases where the ID authority plays a central and transparent role in identity provision.

Business models

Related to the roles and responsibilities of the ID authority are the business models it adopts. In many cases—particularly where ID authorities report to line ministries—ID systems will be financed out of the national budget. However, the digitization of ID systems in particular has created the potential for new business models, including **generating own-revenue by charging fees for identity-related services**, as well as **public-private-partnership** models. Each of these options, along with implications for inclusivity and sustainability are discussed below.

Generating own revenue by charging user fees

ID providers primarily generate revenue through two mechanisms:

1. Charging public and/or private third parties (i.e., “relying parties”) for identity verification and authentication services
2. Charging individuals for certain *luxury services*, such as expedited processing or *optional*, advanced credentials

Such fees can offer some level of autonomy and help isolate ID authorities from short-term fiscal pressures (see [Gelb & Diofasi Metz 2018](#)). **However, while fees may help ensure fiscal independence, and financial sustainability setting them too high may suppress demand and increase exclusion.**



Because identity services are a public good—particularly with respect to foundational ID systems—most services *should be free or with highly minimized fees*, including:

- **Basic credential services for the population:** Charging fees to people for basic identity credentials creates a barrier to adoption. As stated in Principle 2, first copies of birth and death certificates should be free of charge, as should the initial issue of any credential that is mandatory—in law or in practice—to possess for accessing basic rights and services. If fees are charged for certain additional services (such as reissuance of lost credentials), rates should be reasonable, proportional to costs incurred, and transparent to the public. If any fees are to be charged, consideration should be given to subsidizing or waiving them for poor and vulnerable persons.



- **Services for essential or mandatory functions:** For essential government functions that rely on identity verification and authentication services, and/or for public and private sector use-cases where these are mandatory (e.g., for compliance with mandatory SIM registration regulations), the ID authority may hold a monopoly on identity verification and authentication services. In such cases, it is highly recommended that fees be free or minimized. In general, fees should be affordable both for large organizations and for smaller ones, particularly those that serve poor, rural, and other marginalized groups.

The primary users of authentication and verification services are other government agencies—e.g., service providers such as social protection programs, electoral commissions, justice departments, passport agencies, etc.—as well as banks, other financial service providers, mobile network operators, and other entities that need to fulfill KYC requirements. In some cases, these relying parties have dedicated secure connections to the central server and make queries in real time on an ongoing basis; in others, verification is done via web-based portals or APIs. Furthermore, some identity providers conduct large batches of verifications for specific purposes within a set time frame (e.g., periodic deduplication of a voter list before elections). Fees typically vary based on whether the relying party is a public or private entity, the type of data or query, and/or the volume of transactions.

Table 26. Example of fees for verification and authentication services

Country	Public Sector Charge	Private Sector Charge
Argentina 43.8m people US\$14,398 GDP/cap (PPP)	Free	Per query fee: <ul style="list-style-type: none"> ▪ USD 0.125 (basic) ▪ USD 0.375 (fingerprint) ▪ USD 2.5 (biometrics +)
Chile <i>Population:</i> 18.2m <i>GDP/capita USD:</i> 15,346	Free	Per query fee: <ul style="list-style-type: none"> ▪ USD 0.040 (basic) ▪ USD 0.054 (photo) ▪ USD 0.040 (signature) ▪ USD 0.135 (biometric)
Colombia <i>Population:</i> 49.9m <i>GDP/capita USD:</i> 6,408	Free	Fee based on volume of queries, e.g.: <ul style="list-style-type: none"> ▪ USD 0.095/per query for up to 100k queries (biometric) ▪ USD 0.014/per query for up to 12m queries

Country	Public Sector Charge	Private Sector Charge
Ecuador <i>Population: 16.2m</i> <i>GDP/capita USD: 6,273</i>	Free	Per query fee: <i>Webpage based:</i> <ul style="list-style-type: none"> USD 0.15 (biographic) USD 0.30 (biometric) <i>Web service based:</i> <ul style="list-style-type: none"> USD 0.08 (biographic) USD 0.30 (biometric) <i>CD or DVD based (biographic):</i> USD 0.12
India <i>Population: 1.3bn</i> <i>GDP/capita USD: 1,942</i>	Free	Per query fee: <ul style="list-style-type: none"> USD 0.007 (Y/N authentication response) USD 0.30 (e-KYC transactions)
Kenya <i>Population: 48.5m</i> <i>GDP/capita USD: 1,595</i>	Free access to a biographic record and to verify the authenticity of a national ID card.	
Malaysia <i>Population: 31.2m</i> <i>GDP/capita USD: 9,952</i>	USD 0.13 (biographic record) USD 0.25 (biographic + biometric record)	
Pakistan <i>Population: 193.2m</i> <i>GDP/capita USD: 1,548</i>	USD 0.09	USD 0.29
Panama <i>Population: 4.1m</i> <i>GDP/capita USD: 15,087</i>	Free	Fee based on volume of queries: <ul style="list-style-type: none"> USD 1 for 1-10,000 queries USD 0.75 for 10,001-30,000 USD 0.50 for 30,001-60,000 USD 0.10 for 60,001-more
Peru <i>Population: 31.8m</i> <i>GDP/capita USD: 6,572</i>	Free	There are various ways to verify an identity. Wired connections, used by banks, has the following fees: <ul style="list-style-type: none"> USD 0.026/per query for up to 200k queries USD 0.06/per query for 800k or more
Tanzania <i>Population: 55.6m</i> <i>GDP/capita USD: 936</i>	Citizens: USD 0.22 for any query or authentication by government or private sector Legal residents and refugees: USD 1 for any query or authentication	
Thailand <i>Population: 68.9m</i> <i>GDP/capita USD: 6,595</i>	Free access to biographic record in the database and to verify a national ID card	Free access to read biographic data and facial image on the chip of the national ID card (no access to the database).





Source: *Identity Authentication and Verification Fees: Overview of the current practices*. Note: Fees were converted from local currencies to USD using the applicable currency exchange rate on December 29, 2019 and are be subject to change.

Table 26 provides examples of different countries' fee-charging policies and rates for verification and authentication services. These cases demonstrate that fees need not be uniform over time or across users or types of transactions—which can help reduce the burden for some users. Some options for price discrimination include:

- **Pricing based on the user.** To harness the utility of identity services across the public sector, most countries have opted for *lower pricing for government agencies* than private-sector users, with many providing free services for the public sector.
- **Bulk pricing models.** Identity providers, such as **Peru**, **Panama**, and **Colombia**, also offer bulk pricing discounts for frequent users of identity services. **Argentina** and **Malaysia** set different fees depending on the type of data requested, while **Peru** and Ecuador also vary fees based on whether authentication and verification services are performed online or via a hardwired database connection.
- **Phasing in fees.** To ensure rapid up-take by relying parties, one option is to initially waive fees or set prices extremely low, and later increase them if demand is sufficient. In **India**, for example, UIDAI initially kept all authentication services free to lower the barrier to entry for relying parties and has only begun charging relying parties in 2019.

Other important safeguards against overcharging include consultation with a diverse array of potential users as well as independent oversight and regulation. Given that ID providers often have a monopoly on verification and authentication services, a strong regulatory and oversight framework is necessary to help ensure that rates remain affordable and transparent, and that the ability to generate profits does not create perverse incentives for identity agencies. In **Peru**, for example, RENIEC's prices are set *equal to the cost* of the service, as determined by an independent regulatory body. This periodic review has allowed the agency to adjust its fee structure over time, helping to keep prices low and credible. Fees for services to poor individuals are also free of charge and are subsidized by the central government.

Figure 18. Key considerations for charging fees for ID services

 Inclusion	 Data Protection	 Sustainability	 Responsiveness
Basic ID services for individuals (e.g., first credentials) should be free of charge , and other fees minimized; fees for authentication and verification should also be minimized to avoid these being passed on to users	Relying party services that involve data processing must be governed by a comprehensive legal framework to protect personal data and provide the ability of people to see who has accessed their data	Fees can help generate revenue for ID service providers as long as the prices are set at a low enough level to attract users	The process of setting and revising fees should be transparent and involve public and stakeholder consultations

Public-private partnerships

While the public sector will nearly always play a large role in providing government-recognized ID, the scope and mode of private sector participation will depend on the context, needs, and financing constraints. Beyond its role as a user of ID credentials and services—e.g., to fulfill KYC requirements—and a supplier of inputs for ID systems, **the private sector can also be a valuable partner for the government in implementing the ID system itself.** For example, where the private

sector has technical expertise and operational efficiency that government entities lack, governments may outsource certain roles within the ID lifecycle to the private sector in order to reduce ongoing costs—e.g., to provide cloud storage services or a managed call center to handle grievance redress.

However, not all PPPs have been successful, and such arrangements require sufficient oversight capacity, detailed planning, and safeguards to ensure that data collection and identity creation meets the standards set out by the ID authority, that personal data is secure and not misused, and that the system meets the overall goals and requirements set forth by stakeholders. This might include, for example:

- A mandatory authorization process for any companies and their agents involved in the ID system
- The requirement that private-sector provider be located within the country
- Government-retained ownership and control over any data collected and stored by the private sector provider on behalf of the ID system

While there are potential benefits from PPPs to implement an ID system, there are considerable risks regarding their sustainability, unnecessary creation of fees that could lead to exclusion, and potential vendor or technology lock-in. These risks can be mitigated through careful design of the PPPs and transparent, competitive, and accountable procurement processes. Build-operate-transfer models, for example, may create a dependency on a particular vendor if knowledge and resources are not effectively transferred to the government. Likewise, consideration must be given to how the revenue stream for a private partner (e.g. fees for credentials or authentication) could lead to exclusion as discussed above, and the incentive of profits for such concessions could undermine the objectives of an ID system (i.e. to act as a public good to expand access to services).

As discussed more fully in *Digital Identity: Public and Private Sector Cooperation*, **private-sector partnerships could take a number of forms, including but not limited to:**

- **Service agreements.** In the service agreement model, the government contracts with a private firm or firms to undertake a specific role in one or more stage of the digital identity lifecycle. In such cases, firms could receive revenue directly from users or from the government on a performance basis. Whether or not these agreements meet the common definition of a public-private partnership (PPP)—i.e., a “long-term contract between a private party and a government entity, for providing a public asset or service, in which the private party bears significant risk and management responsibility, and remuneration is linked to performance”—depends on the extent to which they are long-term partnerships that require significant investment on the part of the private actor.
- **Build-operate-transfer (BOT) and concessions.** BOT and concession partnerships are ones in which the private sector is *solely or primarily* in charge of building and operating a project, usually for a fixed concession period. These are considered PPPs according to standard definitions, as the contracts bundle together many services and entail significant risk and financing on the part of the private party. In these cases, contracts are often awarded to a single contractor or consortium, project costs and outputs are predetermined, and payment is performance-based and can include a fixed set up cost. Revenue generated by the ID system is allocated between the private and public sectors according to the contract. In BOTs, for example, revenue may go to the government, who then pays the private partner.

In concessions, the private partner collects revenue directly and then pays a portion of this to the government.

Box 25. PPP example in Moldova

Moldova's Mobile eID (MeID, see Box 36)—which provides SIM card-based mobile authentication and document signing—was developed via a **public-private partnership (PPP)**. The partnership involves an agreement between the e-Governance agency (the ID authority), the Center for Special Telecommunications (state-owned Certificate Authority that manages the country's PKI), and two mobile network operators (MNOs) who register end-users in the system.

MNOs are responsible for registration and for providing the technical infrastructure for the MeID, including supplying additional hardware and increasing the network strength. The government was then responsible for integrating the MNO infrastructure with existing PKI infrastructure. Mobile ID implementation took roughly 18 months. The first 12 months were devoted to reaching out to mobile operators, building consensus around a possible PPP model and signing the PPP agreement. Technical implementation took another six months. Since most of the infrastructure investment was made by the private partners, the government did not need to conduct any procurement.

MNOs charge end-users a fee for the use of mobile signatures and the pricing structure can vary depending on specific contract and bundling models, much like air-time, data usage, or text messaging. For example, mobile subscribers who only need a few signatures can opt for a pay-per-use model, while frequent users can opt for bundles ranging from 10 to 1000 transactions. The revenue from mobile signature transactions is split with 85% of revenue going to MNOs, and 15% to the government for the maintenance of the PKI infrastructure.

Source: *Moldova Mobile ID Case Study*





For PPP schemes to attract private sector participation, good policy and credible incentives are needed to offer an enabling environment with a level playing field, a competitive marketplace, a deterministic model for the return of investment, and a system of mutual guarantees. Because each country context is unique, and a **thorough analysis of this context is necessary before adopting a specific partnership model, including careful consideration of the following factors:**

- **Government oversight capacity.** All foundational ID systems require significant public sector capacity. Even where governments are not building and managing ID systems in-house, they must clearly define the roles and responsibilities of different actors and provide the legal and regulatory framework to establish trust and protect privacy and personal data. For partnerships, special legislation may be required—and strong governance practices are necessary—to oversee project implementation and enforce regulations. In contrast, traditional public procurement projects involve well-known and often simpler contracts. However, projects where government officials are involved in operating ID systems—such as in public procurement—may also require significant technical knowledge transfer.
- **Private sector capacity and activities.** The extent to which digital ID and authentication services are already commercially available and interoperable will dictate potential public and private sector use cases and cooperation. The private sector must also have the capacity to provide trustworthy digital identity, offering the same standards of privacy and security protection as those provided by the state, for similar services and in compliance with national privacy regulations (along with international conventions, where applicable, national

sovereignty and governance principles). For example, there is a difference between those companies that are bound by national legislation and privacy frameworks and companies that operate globally but are not obligated to adhere to local privacy laws.

- **Legal and ethical issues.** There may be risks associated with transferring management of a national-level ID system to a private company under certain partnership arrangements. For example, private ownership of public data may not be legal, advisable or socially acceptable, particularly if stored outside the country. For liability reasons, for example, it is generally important for governments to lead the delivery of civil registration, even though these can be facilitated by private sector entities.
- **Sustainability and pricing.** Practitioners should consider the overall estimated costs of the project, estimated volume and demand of digital public services, and the revenue-generating potential for participants. In addition, pay-per enrollment pricing schemes should be structured to incentivize universal coverage for the target population in order to avoid a scenario where certain groups are excluded because registration agents only have an incentive to cover easy-to-reach populations.
- **Vendor and technology lock-in.** In any arrangement, practitioners should structure contracts to help leverage private sector expertise and innovation while enabling interoperability and the long-term flexibility of the system to change technologies and vendors.

Figure 19. Key considerations for private-sector partnerships in ID systems

 Inclusion	 Reliability	 Data Protection	 Sustainability
Where registration is outsourced, fee structures should incentivize universal coverage , including of remote and hard-to-reach populations.	Clear standards and oversight mechanisms must be in place to ensure quality in implementation.	Private companies involved in the ID system must be trusted and subject to national laws regarding privacy and data protection.	RFPs should be structured in a way that ensures competition and avoids vendor and technology lock-in .

Box 26. Additional resources on ID system administration

For more on institutional arrangements, governance, and partnerships, see:

- [Digital Identity Toolkit](#)
- [Identity Authentication and Verification Fees: Overview of Current Practices](#)
- [Public Sector Savings and Revenue from Identification Systems](#)
- [Digital Identity: Public and Private Sector Cooperation](#)

DATA

Foundational ID systems may collect various types of data, as shown in Table 27. The choice of which specific attributes are collected is fundamental to ID system's inclusivity, utility, cost, and trustworthiness, including the extent to which it complies with data protection and privacy standards and good practices (see Figure 20). For example:

- Which data are collected impacts who is likely to be excluded from identification (e.g., some people may not be able to provide certain biometrics).
- The type of data collected will determine the uses and utility of the system for various purposes (e.g., certain use cases may require specific attributes).
- At the same time, the collection of more data than what is needed—including sensitive attributes—increases the cost of registration, creates data protection risks, and decreases the reliability and accuracy of the system over time as non-static attributes (e.g., occupation, education, address, etc.) become out of date.

Key decisions regarding data include:

- What biographic data will be collected and verified, including defining the minimum set of attributes necessary and how to handle sensitive data
- Whether biometric data will be collected, and if so, which types

These decisions will go hand-in-hand with decisions made about the registration process to collect and proof identity data, the types of credentials and authentication mechanisms used, IT infrastructure including data storage, interoperability frameworks for data exchange, and the enabling legal framework and associated privacy and security controls adopted to govern and protect personal data.





Table 27. Types of data and evidence often collected by an ID system

Type	Description	Examples	Use
Biographic	Biographic and other attributes of a person	Name, age, sex, address, nationality	Establishing a person's basic identity attributes; can also be used for deduplication but can be inefficient and inaccurate (e.g., when many people have a similar name)
Biometric	Physical or behavioral attributes of a person	Fingerprints, irises, facial image, signature	Deduplication during identity proofing and/or as an authentication factor

Type	Description	Examples	Use
Supporting evidence	Identity-related documents provided during the application process or vouched by a trusted person	Birth certificate, passport, driving license, voter ID card, utility bill, testimony/letter by a local government official.	Substantiating (“proofing”) a person’s identity during registration
Metadata (collected passively without input from end-user)	Information about data and/or its capture and use, including logging who has accessed the data and when	Name/ID of registration agent, time and location of registration, date/ID of official who accessed data, metadata of the biometric data, checksums	Controlling the quality of data entry, providing context for its collection, creating an audit trail of entry and use

Source: Adapted from the *Digital Identity Toolkit*

Figure 20. Key considerations for the types of data collected

			
Inclusion	Reliability	Data Protection	Sustainability
Certain groups may face technical or practical difficulties providing specific data (e.g., certain biometric modalities) and evidence (e.g., birth certificates or proof of nationality or immigration status), which may deter or create barriers to participation.	Collecting large amounts of data increases information security risks and decreases accuracy and completeness over time as data become out-of-date.	Data protection standards require minimal data collection and purpose limitation in order to minimize risks to privacy and security (e.g., from cyberthreats, function creep, unauthorized disclosure, etc.)	More data fields and strict evidence requirements lead to higher costs and longer registration timelines , including to validate the attributes.

Biographic data

When decided which biographic data to collect, **Internationally-recognized good practice suggests specifying the “minimum set” of identity attributes that uniquely represent an individual.** In essence, the minimum set consists of the *core* attributes used to identify a person by most applications for most purposes. In addition to this data, certain other fields, such as biometric data (discussed in the next section) may also be collected, either to ensure statistical uniqueness and/or for later use in authentication. See Box 27 for examples of minimum data sets.

In some cases—particularly where identification and information systems have been historically weak and there are few reliable sources of data on individuals—countries may be tempted to use the opportunity of building of a foundational ID system to collect lots of personal data for a variety of

purposes (e.g., education status, marital status, household information and income information needed for targeting a social program). In general, however, **it is recommended to keep the number of data fields as close to the minimum set as possible**. Increasing the number of attributes collected will also increase:

- **Time and cost for registration.** Collecting—and then vetting—many data fields will increase the time it takes to register a person and is therefore a major contributor to costs of ID systems. In addition, collecting many data fields will decrease convenience and increase costs for individuals (i.e., more time spent cueing), which can create a barrier to registration.
- **Inaccuracy of data over time.** Any data fields that can change over time (e.g., address) require additional procedures and cost to keep updated and avoid inaccuracies over time. Collecting more non-immutable data fields than necessary (e.g., education, occupation, household information, etc.) therefore increases the probability of inaccurate data and/or the frequency with which potentially costly updates must be done.
- **Risk to privacy and data protection.** Collecting data without a clear use or purpose does not meet international standards on data protection and privacy, including the Fair Information Practice (FIP) principles that data collected must be proportional to the use case and fit for purpose. The more data collected, the greater the privacy risks if that data is compromised.

In addition to the number of data fields collected, countries must also consider the implications of requiring certain biographic attributes, such as potentially sensitive data.

Box 27. Examples of minimum sets of personal data

The **EU's** *eIDAS Implementing Regulation (2015/1501)* established a minimum set of unique identity attributes for an individual for the purposes of basic requirements for mutual recognition of digital identity schemes. *Mandatory attributes include:* (1) current family name(s), (2) current first name(s), (3) date of birth, and (4) a unique identifier which is as persistent as possible in time. *Additional attributes include:* (5) family name at birth, (6) first name at birth, (7) place of birth, (8) current address and (9) gender.

In **India**, to minimize the burden of registration and promote inclusion, the Aadhaar ID system limits the biographic information it collects to an individual's (1) first name, (2) last name, (3) gender, (4) date of birth, and (5) address. Additional biometric fields used for deduplication and authentication include ten fingerprints, two iris scans, and a digital photo.

In **Australia**, the *Trusted Digital Identity Framework: Attribute Profile* (March 2019, version 1.4) defines core identity attributes as: (1) family name; (2) given name; and (3) date of birth. Other data can be collected by identity providers.

Source: Adapted from the *ID Enabling Environment Assessment (IDEAA)*, Australian Government (2019).

Sensitive biographic data

Although all PII can be considered “sensitive” data, certain biographic fields can be particularly sensitive, in the sense that they are personal in nature or might have a serious impact on the individual (*ISO/IEC 29100 Privacy Framework*). When collected or made public, such data could facilitate profiling or discrimination against a person or put them at serious risk of harm. Which

attributes are deemed most sensitive will vary by context, but this typically includes characteristics such as ethnicity, religion, sexual orientation, gender identity, health information, political opinions, criminal convictions and more (see the *IDEEA tool* for further discussion).

Ideally, *foundational* ID systems intended to provide identification for general use should *not* collect and store this type of information because:

- The risk to individuals is high
- The utility of this data for general purposes is low
- The ability of a foundational ID system to keep “sectoral” data accurate and up to date is not as high as those agencies responsible for those sectors
- Extra data fields can add significant cost

There are, of course, certain use cases for which these data are needed and collected as part of a functional ID system, such as a database used to target social transfers to an underprivileged group, or for electronic health records. In such cases, however, separation of purpose should be maintained so that sensitive data is collected and managed separately by an appropriate entity (e.g., the Ministry of Social Affairs, healthcare providers, etc.) rather than the foundational ID provider.

Furthermore, and in line with Principle 6, **ID systems should not disclose this type of sensitive personal information** except for pre-specified and authorized purposes. This means, for example, that these attributes should ideally *not* be programmed into ID numbers or included on cards, as this makes them widely legible and is therefore a violation of privacy. Furthermore, access to individual-level sensitive data by other government actors should be prohibited (ideally) or severely limited and regulated. The decision to collect any sensitive data should be subject to a thorough risk assessment during the planning phase and reflected in the legal framework.



Box 28. Examples of policies regarding sensitive data

Under the **EU's** GDPR, data regarding an individual's racial or ethnic origin would be considered “special category data.” Given the sensitive nature of special category data, the GDPR provides for additional protections to ensure that the processing of such data is lawful. For example, to process special category data, an entity must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9.

In the **United Kingdom**, the Data Protection Act 2018 introduces additional safeguards in relation to special category data. For example, where processing for law enforcement purposes is “sensitive processing,” there must be an “appropriate policy document” in place which explains the procedures for securing compliance with the data protection principles and the periods for which personal data is likely to be retained.

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

Biometric data

In addition to biographic data, many ID systems collect fingerprints, iris scans, facial images, and/or other biometry to use for **biometric recognition**—automatic recognition of individuals based on their biological or behavioral characteristics (*ISO/IEC 2382-37*). This process involves comparing a template generated from a live biometric sample (e.g., a fingerprint or selfie) to previously stored biometric(s) to determine the probability that they are a match.

Biometric recognition encompasses both **biometric identification**—the process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (i.e. 1:n)—and **biometric verification**—the process of confirming a biometric claim through biometric comparison (i.e. 1:1) (*ISO/IEC 2382-37*). These processes can be used to perform two distinct tasks in foundational ID systems:

- **Deduplication of identity records.** To ensure that each person in a database is unique, ID systems can use biometric identification to perform a *duplicate biometric enrollment check*. This involves comparing a template generated from a captured biometric *against all or a subset* of templates stored in biometric database to detect a duplicate registration (a 1:N search), after which the new template is added to the database. This process involves automation as well as manual checks to adjudicate matches.
- **Authentication of individuals.** Some authentication protocols require biometric verification of the user. This involves a one-to-one (1:1) comparison of a template generated from a captured biometric *against a single stored template* (e.g., one stored on an ID card or mobile phone, or in a database).

Biometric recognition has rapidly proliferated in modern ID systems in part because it is currently the **most accurate and efficient technology** available for deduplicating large populations to ensure statistical uniqueness—particularly in countries without existing authoritative sources of identity information—and because it can provide a relatively high level of assurance during authentication. As such, biometrics can be a key ingredient in ensuring the trustworthiness of ID systems.

At the same time, however, biometrics are not required or appropriate in all contexts. In particular, the collection and use of biometric data presents some particular data protection and exclusion risks and can significantly add to the cost of the ID system and add operational complexity. The choice to use biometrics—as well as the particular type of biometric data collected—should be informed by these risks and costs, as well as the objectives, planned use cases, and other constraints to the ID system identified in the planning phase.

Additional analysis on biometric modalities and their use for authentication can be found in the *ID4D Technology Landscape* report. In addition, a more comprehensive ID4D Guide on Biometrics is forthcoming.






Types of biometrics

Countries that plan to use biometric recognition for deduplication and/or authentication can choose from a variety of biometric characteristics (i.e., “modes”). **In general biometrics fall into two major categories:**

- **Biological:** fingerprints, face, iris, veins, etc.
- **Behavioral:** keystroke dynamics, gait, signature, voice, etc.

This section provides a brief comparison of the primary biological biometrics used in national-scale ID systems for biometric recognition. For a more detailed evaluation of some emerging biometric modalities (voice, vascular, DNA, etc.) see the [ID4D Technology Landscape](#) paper.

Table 28. Comparison of biometric technologies commonly used in ID systems

				
		Finger	Iris	Face
USE	Number available	1-10	1-2	1
	Ease of capture	Easy to medium	Medium to hard	Easy
	Adjudication	Medium—requires trained fingerprint examiner	Impossible with naked eye	Easy—any person can compare two faces
	Accuracy for deduplication (1:N) assuming quality capture	Very high depending on number of fingers used and population size	Very high with 2 irises	Low to medium, but improving over time
COST	Capture device cost	1-print (US\$5-40), 2-print (US\$200-250), 10-print (US\$500-750)	US\$ 500-1000	Varies from cheap webcam-type devices to more expensive smartphones/tablets
	Computing for duplicate enrollment check	Medium to high—more complicated algorithms require high-end computer cluster with large memory	Low to medium—iris matching algorithms are the most efficient as templates are stored in binary code	Medium to high—more complicated algorithms require high-end computer cluster with large memory
INCLUSION	Failure to capture (FTC)	<2-5%	~1-2%	~0%
	Children	<6 years: may not be viable >6 years to adult: usable with software that accommodates for aging	<1 year: may not be viable 1-5 years: challenging, requires parental assistance	All ages with updates needed over time (accuracy improves at older ages because the face stabilizes)

Other groups with difficulties	Manual laborers, persons with disabilities, people with cuts on their fingers, people with diabetes	May be more invasive than fingerprints, stigma in some cultures; difficult for persons with visual impairments or albinism	Not always optimized for recognition of darker skin tones, some algorithms have difficulty for persons with albinism
---------------------------------------	---	--	--

Source: Adapted from the *Digital Identity Toolkit* and *Technology Landscape for Digital Development*, and informed by expert consultations.

As shown in Table 28, different biometric modes vary in terms of their:





- **Accuracy.** The accuracy with which the technology matches records. This includes the false match rate (FMR) and false non-match rate (FNMR) of the technology.
- **Universality.** The presence and ease-of-capture of the biometric in members of the relevant population and in a variety of climates and weather conditions. Certain biometrics (like fingerprints) may be poor or damaged among certain groups and can lead to a failure to capture (FTC) a biometric sample or failure to enroll (FTE), as can adverse weather conditions, such as direct sunlight.
- **Stability.** The permanence of the biometric over time (e.g., for children, or the elderly) or after disease or injury.
- **Collectability.** The ease with which good quality samples can be acquired.
- **Usability.** The ease with which individuals can interact with the technology used to capture the biometric data and its utility for different purposes (e.g., some biometric modes may be more convenient for authentication than others)
- **Cost.** The hardware and software costs of collecting and matching samples during initial registration and—if used for authentication—at points of transaction.

In practice, many countries adopt a **multimodal strategy** and collect more than one type of biometric data. This is beneficial for multiple reasons:

- **More accuracy.** More data points (e.g., fingerprints and iris scans or fingerprints and face) help ensure statistical uniqueness to a higher degree of accuracy, which may be necessary in large populations (see Gelb & Clark 2013b)
- **Improved inclusion and fault tolerance.** More modes can help increase the possibility that all members of the population are able to provide a biometric sample (e.g., fingerprints may be difficult to collect for manual laborers, but iris scans may work).
- **Allows for the use of different biometrics (fusion) for deduplication and authentication.** Certain biometric modalities may be optimal for conducting duplicate biometric enrollment checks (i.e., 1:N/N:N matching, while others may be optimal or sufficient for use during authentication (1:1 matching).

The choice of which biometrics to use—if any—will have implications in terms of the trustworthiness and inclusivity of the ID system, as well as potential risks. These issues are discussed below, with particular attention to inclusion challenges, use with children, and concerns regarding privacy and exclusion. Practitioners will also need to make related decisions regarding the technical standards used for biometric recognition, as well as back-end systems used for biometric deduplication.

Figure 21. Key considerations for using biometrics

 Inclusion	 Reliability	 Data Protection	 Sustainability
Certain biometrics may be difficult or impossible for some people to reliably provide , necessitating multimodal biometrics and/or appropriate technical and procedural measures to reduce exclusion.	Biometric deduplication may be the best solution to establish uniqueness in large population, however, not all biometric modes provide the same level of accuracy .	The use of biometrics creates additional risks to privacy and data protection that must be mitigated through legal, technical, and operational controls.	Biometrics can add significant costs to registration as well as the authentication infrastructure.

Challenges for accuracy and inclusion

In deciding the set of biometrics to use, special attention needs to be given to the ability to collect these characteristics from the entire population. For example, there are specific groups and conditions—both of which may be overrepresented in developing countries—where FTE errors during enrollment and FNMRs during biometric verification are likely to be more common. Where individuals are unable to enroll, or where authentication procedures fail to confirm that a person is who they claim to be, this will lead to exclusion.

There are **three categories of people** that present difficulties for biometric recognition, including:

- People who *cannot physically provide* an acceptable biometric (e.g., amputees, survivors of leprosy, etc.) to enroll in the first place
- People for whom *acquiring reliable biometric samples is difficult* (e.g., manual laborers, elderly people, children, people with visual impairment, persons with albinism, etc.) which could make enrollment or authentication difficult
- People who *decline to provide* their biometrics (e.g., because of religious or cultural constraints, such as the appropriateness of data capture techniques that require physical contact to get accurate readings)

In addition, there are **other factors that can lead to accuracy and inclusion challenges with biometric recognition**, including:

- *Environmental and procedural issues:*
 - Harsh conditions, such as direct sunlight, excessive wind, dust, humidity, and dryness, etc.
 - Minimal training or low capacity of the operator capturing the biometrics
 - Lack of incentives and/or time for capturing quality data
 - Poorly implemented enrollment and quality assurance process
- *Biometric system characteristics:*
 - Quality of the biometric scanners and software, including the Automated Biometric Identification System (ABIS) and other software development kits that may be used
 - The statistical nature of biometrics
 - Changing properties of biometric characteristics (i.e., facial appearance over time)
 - Non-optimum threshold setting for matching algorithm—i.e., the tradeoff between the FMR and FNMR

Some of these issues may be addressed through:

- *Designing a multi-biometric system* (see above) to ensure that most people are able to provide at least one viable sample
- *Optimizing enrollment procedures*, including by using:
 - a. Better capture devices and software with built-in quality assessment to improve data quality and reduce FTE
 - b. Quality Assurance Process and standards (e.g. NFIQ-II)
 - c. Conditioning materials (gels, alcohols, etc.) that improve finger image contrast
 - d. Uniform background for facial images
 - e. Choice of capture devices (small versus large scanners, 4-4-2 versus single fingerprint scanners, optical versus capacitive)
- *Implementing comprehensive training of operators* to ensure understanding of and adherence to protocols

To ensure the inclusion of this group, it is vital that the identity provider develop transparent and practical methods of exception handling. For duplicate biometric enrollment checks during registration, this could involve identity proofing by other means, such as witnesses, alternate documents, demographic deduplication, and more. For authentication, there must be alternative methods of proving someone's identity when biometric verification fails or is not possible, in order to ensure that people are not denied access to rights and services for which they are eligible and entitled. Exception handling procedures must be complemented by strong grievance redressal mechanisms to ensure that no one is excluded or unfairly treated as a result of the ID system. This is also true for any other type of authentication method and is not limited to the use of biometrics.

Children and biometrics

One persistent inclusion challenge with ID systems that use biometrics is that many biometrics take time to develop or stabilize after birth. For example, the viability of the following modes depends on age (see also Table 28):

- **Fingerprints (6+ with update).** The papillary ridge structure does not develop before the age of six, which means that reliable fingerprint minutiae—the points of comparison in a biometric template—are difficult to extract before that age. Furthermore, aversion to the capture process (i.e., squirming) makes it difficult to collect quality samples.
- **Iris (~1-2+).** The iris is fully formed 1-2 years after birth but poses some difficulty in capture and requires significant assistance from the parents until around five years of age.
- **Photos (0+ with updating).** Images of the face can be captured from birth, but they need to be updated frequently in the first years of life in order to be useful for automated recognition.

Given that it is currently not feasible to capture stable biological biometrics at birth—nor are there yet clear use cases as part of a foundational ID system—countries have a few options for the use of biometrics for children in an ID system. The first option is to enroll young children without biometric information—or with information that will change over time—and either add or update this information at a later date (e.g., at the first year of high school, for practical reasons). A second option is simply to only include older children and adults in the ID system. Typically, such solutions also include linking the child’s record with their parents (see Box 29), which can also help establish statistical uniqueness of a child at the point of birth registration.

Box 29. Examples of incorporating children into an ID system with biometrics or alternative methods of establishing uniqueness

In the **Indian** state of Haryana, children are enrolled in Aadhaar using a parent’s number which is biometrically authenticated. The biometric data for the child must be uploaded when they turn five years old, and the identity re-registered at age 15. **Peru’s** ID system also collects infant biometric information (such as footprints and a photo) in combination with parent’s fingerprints.

Countries may also implement a mandatory renewal period in order to update children’s biometrics and other information. In **Argentina**, for example, children are required to renew their ID at age 8.

Indonesia’s population register (SIAK) covers all ages, however biometrics are collected at age 17 (or younger for married women) for the issuance of a national ID smartcard (e-KTP). A child’s identity record is created—and a unique ID number (NIK) assigned—at the time of birth registration, which is also when the child is included in the parents’ or guardian’s family registration book (KK) and a moment when the Ministry of Home Affairs checks if the child may have already been registered in the same KK (i.e. deduplication). A child ID card (KIA) is optional at any age up to the age of eligibility of an e-KTP.

Source: Adapted from the *Digital Identity Toolkit* and *Argentina Case Study (forthcoming)*.

This is an area where technology is potentially changing fast, and companies and researchers are working to develop and test biometric capture devices specifically tailored for infants (e.g., foot geometry and ear shape).

Privacy concerns for biometrics

The processing of biometric data—whether in raw image or template format, and whether encrypted or not—must be subject to the same legal, procedural, and technical controls used to protect other types of sensitive PII. In addition to the general risks of processing any type of PII, however, there are some **particularities about biometric data that introduce additional privacy concerns**, including that:

- Some additional personal information may be extracted from certain types of biometric data (e.g., gender, race, age, etc.)
- If biometrics are compromised, they cannot be reissued like cards, passwords, or PINs—i.e., you only have one right index finger
- Biometrics are uniquely linkable to a person, increasing the potential for correlating data about an individual
- The ability to collect biometrics passively (e.g., through photos or video images) requires safeguards to protect consent

While legal measures (e.g., prohibiting the use of biometrics collected for the ID system for unauthorized surveillance or forensics) and technical controls (e.g., encryption of biometrics when stored and in transit) can improve the security of this data, no system is foolproof. For example, even if biometrics are stored as encrypted templates in order to eliminate the possibility of a thief accessing the original images, there is still the possibility that synthetic biometric images can be reconstructed from templates (see, for example [Chu et al. 2012](#) and [Cao & Jain 2015](#)). (For this reason, keeping centrally-stored biometrics as templates does not substantially increase security; conversely keeping centrally-stored biometrics as images has additional benefits, such as the ability to generate new templates with a different algorithm). With improvements in artificial intelligence (AI) and machine learning, the ability to spoof biometrics is likely to become easier over time.

Therefore, although it may be more difficult to steal a biometric than a password, the potential consequences of this theft—e.g., the inability to reissue a biometric and the inherent linkability of the data—may be more severe. Practitioners must fully weigh these risks against the potential benefits of using biometric recognition.

IT SYSTEMS

ID systems are built on strong IT infrastructure, including computing resources, hardware, applications, network and server architecture, and more. The IT architecture that knits all these technologies together is a critical determining factor of the reliability, security, and flexibility, with major implications for program cost, sustainability, suitability for different use cases, the ability to protect personal data, and the adaptability of the system over time.

Devising an IT architecture that balances all these factors effectively is a major undertaking, requiring expert input from technologists, ID practitioners, and other stakeholders. This Guide cannot consider every factor in detail or provide a formula for determining the correct architectural choices. Rather, this section attempts to present an overview of key decisions that practitioner's should be prepared to take in respect to:

- Hosting options for data, services, and related applications
- Applications and software (*coming soon!*)

Hosting options

Significant computing resources are needed to store and process identity data (e.g., in response to identity verification queries), and there are multiple options for hosting this infrastructure. Key decisions include:

1. **Who operates the physical facilities (“datacenters”)** that house the IT infrastructure, providing power, cooling, physical security, network connectivity, etc.—the ID authority, another government agency, or some form of private sector provider.
2. **Whether the infrastructure itself is dedicated to the ID system** (so-called “single-tenant”) or part of a pool of shared resources, available on-demand to multiple clients (so-called “multi-tenant” or “cloud” computing).

In particular, practitioners should evaluate the following solutions for ID-related hosting in light of system requirements and country context:

- **Dedicated datacenter operated by the ID authority.** Some countries choose to host data and applications in-house through the use of dedicated datacenters. This option gives full control over all components of the ID system, including physical facilities and access, hardware, software (operating systems, applications, technical services), and data. However, it also requires the ID authority to take on significant responsibility and all capital and operating expenses for those components, as well as ensuring the presence of technical expertise needed to support the ongoing operations and maintenance. It could also be an unnecessary duplication of an existing shared datacenter operated by a central IT ministry or similar agency in the country, if such exists.
- **Shared datacenter operated by another government agency.** Another option is to use a datacenter run by a central IT ministry or similar agency that provides shared hosting services

for multiple government agencies (and sometimes also the private sector). Costs for this solution are typically lower than running the in-house datacenters because of the scale advantages in sharing capital and operating costs. The operator will often offer additional services (such as server maintenance and patching, backup and restore, etc.) with similar economies of scale. There are security and resilience implications of the multi-tenant model, since the underlying infrastructure is shared with other clients. These are discussed in more detail below. A shared datacenter typically supports three broad models of provision:

- **Colocation.** In this model, the shared datacenter provider offers space, power, physical security and network connectivity. The ID authority provides and configures and operates its own the infrastructure (servers, storage). Accordingly, the authority bears the capital cost of its infrastructure, the allocated charge for power and space, and the staffing and running costs for operations and maintenance.
 - **Managed hosting.** In this model, the datacenter provides and operates the IT infrastructure as well as the physical facility where it resides, in a “single tenant” configuration designed for and dedicated to the ID authority. The provider will either charge an up-front capital cost for this infrastructure or use a leasing model with a specified minimum term. A regular service charge will cover operations and maintenance. Limited flexibility to increase or decrease the dedicated capacity over the term of the contract may be built in.
 - **Government (“private”) cloud.** In the cloud model, the datacenter operator is also responsible for all physical facilities and IT infrastructure but uses modern “virtualization” technologies to pool this infrastructure and make it available on a flexible, pay-by-usage basis to multiple clients (known as “Infrastructure-as-a-Service” or IaaS). Cloud operators often offer additional service layers such as databases, authentication services or analytics platforms (so-called “Platform-as-a-Service” or PaaS). There is no up-front capital cost, while all the operating and maintenance costs of the underlying infrastructure are included in the pay-by-usage charges. This model is also extremely flexible, allowing the authority to provision (or de-provision) required infrastructure capacity very rapidly, and pay only for what it uses (with charges by the second in some cases). In return, the authority sacrifices control over the configuration of the underlying hardware and must choose from a menu of infrastructure configurations offered by the cloud, which may not support some applications with specific infrastructure requirements.
- **Shared datacenter operated by commercial organizations.** Private sector firms also offer infrastructure hosting on the same models just described—colocation, managed hosting and multi-tenant cloud. They operate in very similar ways to shared government datacenters but are likely to serve a wider range of public and private sector clients, with a correspondingly wider range of services (some private sector operators also have datacenters tailored and restricted to government agencies.) In addition, the physical location of the datacenters is in most cases outside of the country, and the data stored may migrate across datacenters depending on a number of factors independent of the contracting authority. There are also so-called “hyperscale cloud” platforms—such as Amazon Web Services, Microsoft Azure and Google Cloud Platform—from specialists in the multi-tenant model that have multiple data

centers across continents with high-capacity networks connecting them to each other and to the wider internet. Because of their scale they can offer a very wide range of IaaS and PaaS options and can also provide replication of data and infrastructure across geographies to support highly resilient, highly accessible large-scale applications. As these platforms are open to any client able to pay, they are known as “public” clouds.

- **Hybrid approaches.** It is possible to combine different elements of the models described above in a hybrid solution. For example, a government datacenter could be used for core storage (e.g. sensitive and restricted data) and compute provision, with flexible hyperscale public cloud capacity added to meet peak demands on the system; or commercial managed hosting could be used for the current “production” solution, with cloud capacity used for development and testing of new features and applications. (A hybrid approach that combines clouds from multiple providers is also known as “multi-cloud”.) Hybrid hosting strategies are very common in commercial IT, as they have the potential to offer a “best of all worlds” solution. However, there is clearly added technical and commercial complexity in managing multiple infrastructure models with multiple providers; this needs to be balanced against the benefits.

Some key differences between these options are summarized in Table 29.

Table 29. Comparison of data storage options

Option	CAPEX	OPEX	Required staff	Control over infrastructure	Elasticity & flexibility	Network & connectivity	Data location
Dedicated, agency-owned data center	Most expensive, includes cost of equipment and datacenter facility (building, fire protection, power etc.)	Most expensive, OPEX for equipment and datacenter expenses, including staff	Datacenter, network, physical security, server/system administration, application/database administration, cybersecurity	Full control over data and all components of the infrastructure	No elasticity, least flexibility in provided services	Good LAN connectivity required (and good G-NET connectivity required for data sharing)	On premises
Shared datacenter – collocation (government and private)	CAPEX for equipment collocation	OPEX for collocation costs and own equipment	Server/system administration, application/database administration, cybersecurity	Control over data and collocated equipment	No elasticity, least flexibility in provided services	Good G-Net connectivity required	In country
Shared datacenter – managed hosting (government and private)	CAPEX for infrastructure and equipment are typically born by the datacenter provider but it can vary by provider	OPEX for managed services	Application/database administration	Limited, as provided by the contract	Limited, as provided by the contract	Good G-Net connectivity required	Typically in country

Option	CAPEX	OPEX	Required staff	Control over infrastructure	Elasticity & flexibility	Network & connectivity	Data location
Government cloud	No CAPEX for the ID authority, costs are born by cloud operator	OPEX for resource usage (pay per use model)	Application/ database administration	Control over data and own applications	Elastic. Some flexibility in service availability	Good G-Net connectivity required	In country
Private-sector operated public cloud			Application administration	Control over data	Elastic. Flexible service availability	Low latency required for business-critical systems (e.g. fintech)	Anywhere the provider is operating datacenters
Hybrid cloud			Application/ database administration	Control over data and own apps	Elastic. Most flexibility in service availability	Good G-Net connectivity required	Sensitive data stored in country; other data stored in private-provider datacenters with a global scale/footprint

The appropriate choice of a data storage solution will depend on a number of factors, including:

- **Existing infrastructure and service providers:** The viability of any particular data storage strategy or solution depends, foremost, on the availability or existence of dedicated datacenters and trusted government and/or private-sector provided datacenters and cloud services. If an in-house datacenter does not already exist, building one will be a major expense for the ID program and will take some time to build (e.g., potentially several years, depending on procurement procedures, required authorizations, existence of powerlines, connectivity etc.). At the same time, it may be the only option if shared datacenters and/or cloud services are not available or desirable for other reasons. When data storage is contracted to a government IT agency or a private-sector provider, is it essential that the service provider offers appropriate service-level-agreements (SLAs) to meet the needs of the ID authority.
- **Storage and processing capacity and elasticity.** Data storage services must have enough storage capacity and processing power to meet demand, both during high-volume start-up (e.g., mass registration), peaks in demand (e.g., around cash transfer distribution dates), and medium- to long-term growth (i.e., as a function of population size and the expansion of services). A primary advantage of cloud services is that it offers the flexibility to automatically add or remove computing resources when needed to meet requirements. In contrast, datacenters require purchasing enough equipment to handle spikes in usage; however, at low-volume periods most of this equipment sits idles for as much as 90-95 percent of the time. At the same time, depending on the technical specifications and service requirements, cloud hosting may not be the best solution for certain functions that require dedicated high-capacity computational processing power, such as an Automated Biometric Identification System (ABIS), which is extremely resource intensive. In these cases, it is possible for an ID authority to store most of its other functions that do not have such high computational processing requirements (e.g. database, core software and the authentication system) on the




cloud, while the ABIS and its biometric libraries are stored on a smaller, dedicated data center.

- **Cost and budgeting:** Datacenters have higher capital expenses (CAPEX) for the ID provider than cloud services, and also have higher ongoing costs related to staffing. As described above, optimal performance for a datacenter requires paying for equipment that is often idle; while cloud services offer a pay-for-use model. At the same time, this means that the monthly or annual operating expenses (OPEX) of datacenters are more regular than for cloud services, which can be highly volatile due to fluctuations in activity. Therefore, although cloud computing for ID systems may help optimize resources, it is only feasible if the authority's budget and business model can accommodate variable expenses. Under that model, the budget allocated to the ID authority has to be agreed upon and negotiated with Government to ensure yearly appropriation to sustain the service.
- **Connectivity.** Transferring and updating data in an ID database requires sufficient digital infrastructure to connect to the datacenter and/or cloud—in terms of both speed and reliability. Private-sector provided cloud services in particular requires very fast, regular network connections. If network infrastructure is unreliable or is already highly utilized, cloud-computing may be too much of a burden, causing applications to crash or be inaccessible. In such situations, a private cloud on a dedicated line could be considered, but a private or hybrid cloud would be unviable without infrastructure upgrades. In the case of biometric verification, high-speed broadband connectivity is needed to ensure the software applications used for matching algorithms perform robustly, reliably, and securely.
- **Control and location of data.** All of the solutions described above provide control over data; however, they vary with regard to control over equipment and applications (highest with in-house datacenters, lowest with private clouds). In addition, government-provided hosting solutions, including in-house datacenters, shared datacenters, and private clouds, data will remain within the territory. In contrast, data stored in a public cloud or the public portion of a hybrid cloud may be stored in multiple locations abroad. Where a country prohibits the transfer and/or store certain data (e.g. health, tax, personal data etc.) abroad, this will make these options unviable. A hybrid cloud could still be viable provided that data resides within the country and additional services (e.g. anti-DDoS, load balancing, etc.) are contracted from the public cloud provider(s). At the same time, it is important to note that storing or transferring data abroad does not necessarily increase security and privacy risks, and in some cases keeping a back-up off-site (as **Estonia** does) could help mitigate the effects of severe data loss events. It is important to understand the backup and disaster recover processes and policies used by the cloud provider so that the contracting agency is fully confident of the reliability, security, and privacy of the cloud provider.
- **Application dependencies:** Applications that depend on specific hardware—such as a particular chip set or an external device such as a fingerprint reader—might not be a good fit for cloud-based services, unless those dependencies are specifically addressed. Similarly, if an application depends on an operating system or set of libraries that cannot be used in the cloud, or cannot be virtualized, that application cannot be moved to the cloud. In particular, public cloud operators generally provide very little customization to accommodate specific tenants, so application development requires focusing on applications that can be run from a cloud environment.

- **Security and data protection:** No matter the solution, the data host must have sufficient capacity—including staff, policies, operating procedures, and technology—to protect personal data from unauthorized access, misuse, loss, or theft. This includes physical and cybersecurity measures and disaster recovery mechanisms. Putting data on a public server accessed over the open internet—as occurs in both public and hybrid cloud models—is inherently riskier than hosting in datacenters or private government clouds that are not connected to external networks, although connections to the ID system could still be configured via secure VPN channels. At the same time, major private-sector cloud providers typically have advanced protections against internal and external threats, follow best-practices security protocols, and have multiple data centers to provide automatic backups. In contrast, many government cloud and datacenter providers may have smaller dedicated security teams. However, it is often believed by some that placing sensitive data and platforms in the cloud is by default more secure than local hosting. This is a misconception; cybersecurity arrangements for cloud hosting are simply different from those made locally and need to be implemented just as carefully and by design. While it may be true that placing data in the cloud and partially outsourcing cybersecurity arrangements ultimately lead to a more secure platform in some countries with low cybersecurity capacity, inadequately secured data centers and weak processes, it would be inadvisable to assume so in every case. A reputable vendor's arrangements, risk tolerance, and response procedures should be evaluated carefully and regularly and designed to align with good practices prior to data upload.

For a deeper assessment of when and how to use cloud computing for IT systems in general, see the World Bank's Cloud Readiness Toolkit Assessment (*World Bank 2016a*).

Figure 22. Key considerations for data storage

 Reliability	 Data Protection	 Sustainability
Data must be secure and have adequate back-up and disaster recovery to prevent data loss.	Data storage solutions must provide adequate data protection and security measures to prevent unauthorized access and protect against cyberattacks.	Data storage choices will have a potentially large impact on start-up and/or operating costs ; data storage solutions must be flexible enough to adapt to long-term needs .

REGISTRATION & COVERAGE

Registration—including who is eligible to enroll, how people are enrolled, and the technology identity proofing process—is a critical component of ID systems. Few projects compare in terms of scale and complexity to a foundational ID system's initial mass registration. It requires contact with every (or nearly every) person in a country and the collection of sensitive data. Any negative experiences—e.g., long queues, denial of registration, personal data being lost or stolen—can quickly turn public and media sentiment against an ID system and undermine a significant investment. Conversely, a successful mass registration drive can also generate a positive feeling of national mobilization. Likewise, the speed that universal or high coverage can be reached determines when use cases can go live and therefore when the benefits of an ID system are realized or perceived. It is therefore important for countries to take time to carefully and comprehensively plan their initial mass registration. Finally, the sustainability of an ID system also depends on how it continuously enrolls people as they are born in or migrate to the country.

Fundamentally, foundational ID systems should aim for universal access for the entire resident population (and potentially nationals living abroad) and for a user-friendly registration process that allows for quality identity proofing. Implications for registration include the following:

- Who is eligible to enroll in the system has direct implications for inclusion and the system's ability to meet goals such as legal identity for all (SDG target 16.9) and the needs of particular use cases (e.g., providing universal health care, KYC for financial account opening or SIM card registration, voting, etc.).
- Registration strategies—including where, when, and how people apply for an ID—can also create or remove barriers to participation in the ID system, impacting coverage and people's overall experiences with and trust in the system.
- Identity proofing will impact the overall accuracy and trustworthiness of the identities (i.e., the potential level of assurance they will provide during authentication), as well as the cost of the system.

This section covers key decisions related to registration and coverage, including:

- **Eligibility.** Who can access the ID system, including nationals and non-nationals, and beginning at what age.
- **Registration strategy.** The broad approach for data collection for the initial mass registration and continuous registration.
- **Registration operations.** The process, staff and equipment for carrying out registration.
- **Identity proofing.** How data will be validated and identities deduplicated.

These activities are highly contextual, and practitioners will need to carefully weigh multiple factors when designing registration requirements and processes.

Eligibility

Along with the type of data to be collected, determining who will be eligible to register in the ID system is a first-order decision with implications for the inclusivity, cost, utility, and overall development of the system.

Inclusion of non-nationals

In line with various international commitments made by countries to provide proof of legal identity to all people who reside in their jurisdiction without discrimination—particularly SDG target 16.9 to provide legal identity to all by 2030—countries should make foundational ID systems accessible to all resident non-nationals. While resident non-nationals—including migrants, refugees, asylum seekers, and stateless persons—will not be a large proportion of the population in most countries, they are often among the most vulnerable and need access to services and the ability to exercise their rights just as much as nationals. The denial of access to an ID system that is frequently required for access to rights, services, and opportunities can therefore lead to their marginalization.

Restricting a foundational ID system to only nationals can also be exclusionary for many people who *are* nationals but are unable to prove this. This is particularly the case in *jus sanguinis* countries, where—in contrast to *jus soli* countries that recognize citizenship for anyone born within their jurisdiction—nationality determination requires more than documentation of a person's birth location (e.g., it may also require documentation of parental nationality). Poor people tend to lack this documentation at higher rates, as do other marginalized groups such as ethnic minorities or those living in border areas who may previously been discriminated against and denied citizenship. Therefore, ID projects that require people to prove their nationality in order to access ID run serious risks of disenfranchisement and exclusion.

There are two ways that a country can include resident non-nationals in a foundational ID system:

1. **Not making any distinction between nationals and non-nationals:** Through this pragmatic approach, eligibility is exclusively based on a person having resided in a country for a certain period, and no data about the nationality or legal status of the applicant is collected. Importantly, this type of ID system does not ascribe any rights or entitlements, including to nationality or legal status and therefore is insufficient to provide authorization for certain purposes (e.g., voting). As part of this separation, these statuses must then be managed in other systems by relevant authorities with a legal mandate (e.g., an immigration agency) using the foundational ID as a source of trusted identity information and authentication (e.g., as a layer on top of the foundational ID system). This approach has a benefit of greatly simplifying the registration process, which could in turn significantly reduce the cost and time for registration. A notable example is **India's** Aadhaar system (see Box 30).
2. **Making a distinction between nationals and non-nationals, while ensuring universal access and respect for rights:** It could be that—due to the use cases of the foundational ID system or political dynamics—option 1 is not feasible. If a distinction based on nationality must be made, it is important that resident non-nationals do not face unnecessary barriers accessing the ID system and that their rights—particularly to non-discrimination and privacy—

are protected. For example, requiring a residence permit during Identity proofing could exclude some refugees, stateless persons or irregular migrants who live in a country and who could have been born there. The requirements for registration should therefore be minimal. Likewise, issuing non-nationals with an ID number, card, or other credential that makes it visible that they are a non-national could lead to discrimination—instead, this attribute could be “hidden” in the database and/or the chip of a smartcard, and made accessible only to those who need access such as immigration authorities (see Box 30 for an example from the **Philippines**). If the ID system is intended to provide legal proof of nationality, then it is critical that there are sufficiently accessible and transparent grievance and appeal processes for people whose claim to nationality might be rejected, and for people to be able to easily transition from the non-national category to the national category.

Box 30. Country Experiences with ID and Nationality

In **India**, the Aadhaar system is accessible to every “resident” of India, defined by the *Aadhaar Act* as “an individual who has resided in India for at least 182 days in the last 12 months.” No data on the nationality or residency status is collected. In a country with complex nationality laws and procedures, this simplification of the foundational ID system is a significant reason why it managed to register more than one billion people in less than six years. However, there have been instances where police or other authorities have mistakenly arrested non-Indians in possession of an Aadhaar number or card for allegedly fraudulently obtaining Indian nationality, which highlights the need for effective awareness raising of what a foundational ID system is and is not.

In the **Philippines**, the Philippine identification system (PhilSys) system will be accessible to anyone who has resided in the Philippines for longer than 180 days. Unlike Aadhaar, however, it collects information about whether an applicant is a Filipino national or not—and, importantly, it does not collect what the other nationality might be. This information is not printed on the ID card nor is evident in the holder’s ID number, but it may be shared if legally required and consented. In order to reduce the complexity of registration, the *PhilSys Act* states that the PhilSys does not provide incontrovertible proof of Filipino nationality, because this determination is the mandate of the Philippine Bureau of Immigration.

Source: Adapted from the *ID Enabling Environment Assessment (IDEAA)* and expert consultations with World Bank staff.

Inclusion of children

Ensuring that children have proof of their legal identity is fundamental for ensuring their rights, protection, and access to services, such as enrolling in school, receiving public benefits, and preventing child trafficking, labor, and child marriage. For this reason, ensuring universal birth registration, as required by SDG 16.9, is a fundamental priority in any country.

In addition to a birth registration, children can also be included in other ID systems. Traditionally—both because of the rights and duties that come with attaining the age of majority in many countries, and because legal identity should be provided to children through the birth registration and certification process—national ID systems have only covered the population above a certain age, such as 16 or 18 years old. However, a growing number of countries have begun to extend foundational ID systems to children (often optionally), either by linking the issuing of a unique identity to birth registration and/or by making (often optional) “child IDs” available at a younger age (see Box 31). While clearly not a substitute for birth certificates, providing unique identities and/or credentials

to children may be useful in certain instances. For example, many digital ID credentials are more portable and have superior security features (e.g., such as a photo) than the paper birth certificates issued in many countries. In addition, digital credentials offer some added functionality, such as the ability to transact at a higher level of assurance, which may make it easier for young adults access to SIM cards and other resources. At the same time, children typically do not engage in many transactions without the assistance of adults, so the added value of advanced credentials may be reduced.

However, the collection of data about children raises unique data protection and privacy risks, including in relation to consent and biometric capture. Children are more vulnerable than adults to identity theft and other privacy violations because they are less equipped to verify and monitor the accuracy and use of data about them, and such identity theft can go unreported for extended periods of time. Consent depends on the parent(s) or legal guardian(s), which must be recorded (but able to be removed when the child reaches the age of majority). Children without parents or legal guardians present at the time of registration can be complex cases that need to be dealt with in accordance with relevant laws on child protection. While biometrics can be captured as young as five years old, they will need to be recollected later at 15-18 years old when physical growth has stabilized. Furthermore, the collection of biometric data from children raises special practical and ethical considerations (more analysis forthcoming in UNICEF-World Bank publication on children biometrics). As an alternative to biometrics, the uniqueness of a child's registration (including enrollment through birth registration) can be based on the unique identity of the parent(s) or legal guardian(s) (excerpted from *IDEEA*, see full text for more).

Box 31. Examples of the inclusion of children in ID systems

Belgium: An-eID card is compulsory for nationals from the age of 12. Children under age 12 may obtain a Kids-ID card (issued to the person with parental authority over the child), and this is compulsory for children under 12 who travel abroad. The Kids-ID card contains a safety feature which provides contact numbers in case of emergencies. The reverse side of the Kids-ID contains a hotline number that uses the child's identification number to link automatically to the telephone number of one of the child's parents or another relative. Parents may also provide up to five additional contact numbers, classified by order of importance. If there is no response to any number on the list, the call automatically goes to an agency for missing children. The Kids-ID contains an electronic chip designed to protect children on the Internet by enabling them to identify themselves in chat rooms that are reserved for children.

India: Children may be registered in the Aadhaar program from birth, but no biometrics are captured for children under age five. Their Aadhaar number is processed on the basis of biographic information and linked to their parents' Aadhaar numbers. A facial photograph is taken for manual identification when needed. Children can re-enroll when they reach age five with ten fingerprints and iris and facial photographs. The biometric data is updated once they reach age 15.

Indonesia: Beginning in 2016, optional Child Identity Cards (*Kartu Identitas Anak* or KIA) have been issued to newborns along with their birth certificates and to children of older ages. There are two categories of identity cards for children: one for children under 5 years old (without a facial photograph) and another for children between the ages of 5 and 17 years old (with a facial photograph). The KIAs are automatically changed into Citizen Identity Cards (*Kartu Tanda Penduduk* or KTP) at age 17 (or younger for a married female), but the identity number does not change.

Malaysia: “MyKad” ID cards are issued at age 12 and updated at 18. Children below age 12 may apply for non-compulsory “MyKid” ID cards. The MyKid card, unlike the adult MyKad, does not record a photograph or a thumbprint but contains a chip with information about birth, health and education.

Thailand: Thailand assigns a personal ID number (PIN) on a child’s birth certificate. When the child turns seven years old (also the first year of compulsory education), they are required to provide four fingerprints and their facial image and will receive a national ID card. The fingerprints and facial image are recaptured at every subsequent issuance of a national ID card.

Uruguay: A *Cédula de Identidad* (identity card) is compulsory from birth. Enrollment takes place at birth, and parents must obtain an identity card for the infant within 45 days. A thumbprint is taken at enrollment. However, because of the difficulty of using the fingerprints of newborns for matching, this biometric information is initially stored but not used for identity validation or de-duplication. When a child reaches age five, a complete set of ten fingerprints is taken and stored as the basis for identity validation.

Source: Adapted from the *ID Enabling Environment Assessment (IDEA)* (see publication for full sources) and expert consultations from World Bank staff.

Inclusion of nationals abroad

Countries may choose to make an ID system accessible to nationals who reside in other countries. The key benefit of covering nationals abroad in a digital ID system is that they will be able to access various e-services—e.g., filing taxes and registering or transferring property—remotely. The decision of how registration in the ID system is conducted, and which other services are offered, will be contingent on budget, since it is expensive and logistically challenging to ship equipment overseas, including to embassies and consulates. However, the ID authority may be able to justify charging certain fees to nationals abroad to recover these costs where these do not exclude people from accessing services. Alternatively, an ID authority can set up registration points at border crossing so that nationals who ordinarily reside abroad can register and pick up credentials when they are traveling to or from the country.

Registration strategy

Once practitioners have determined which data are needed for the ID system and who is eligible, the next step is to determine how data will be collected—i.e., how people will register in the system. One of the most important considerations is the timeframe for which the country wants to reach universal or near universal coverage of the ID system.

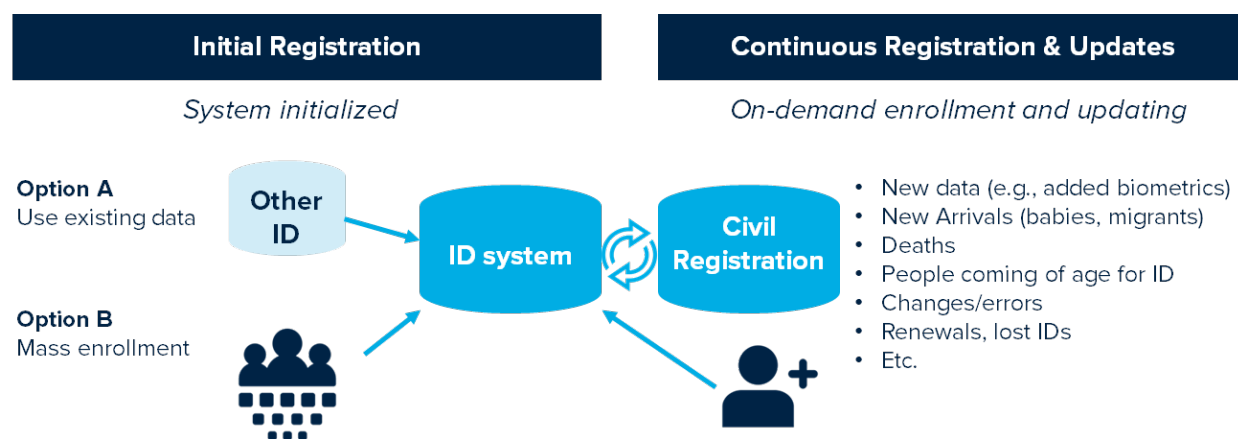
Registration strategies, modalities, and timelines have critical implications for the coverage and inclusivity of the ID system and the quality and accuracy of the data collected. Furthermore, the interactions between registration agents and the population are vital points of contact that can either foster or weaken trust in the system. Therefore, registration processes should be designed with the goal of ensuring:

- **Universal coverage** of the population, with particular attention to the “last-mile” people and communities that may be difficult to reach and are therefore at risk of being left behind
- **High quality data** that is accurate, complete, updated over time, and meets required standards

- **Positive registration experiences** for people and operators with procedures that are accessible, transparent, and free from discrimination or undue burdens

Typically—and for countries rolling out a new foundational ID system in particular—it is necessary to adopt a “stock-and-flow” approach to registration in order to ensure inclusion of the entire existing population (i.e., the stock of people already living in the jurisdiction) as well as the continuous flow of new people (e.g., newborns and immigrants). As shown in Figure 23, this involves multiple channels of registration, as well as linkages with the civil registration system, throughout the continuous operation of the ID system.

Figure 23. Registration strategies for different stages of the lifecycle



In particular, practitioners have a number of interrelated decisions to make with regard to:

- Approaches to initial registration
- Approaches to continuous registration and data updating
- Insourcing and outsourcing
- Generating demand for the ID system

Each of these topics and their implications—particularly for inclusivity, data quality, and costs—are discussed in more detail below.

Approaches to initial registration

When introducing a foundational ID system (or upgrading an existing one), countries typically rely on one or both of the following methods to cover the existing population (i.e., the stock):

- **Leveraging existing registries and databases.** If a country has one or several existing registries or databases—e.g., an older foundational ID system and voter registry—that holds the same data as what will be stored by the new ID system, then this data could be migrated and harmonized. However, for this approach to work, the data should be of a satisfactory quality, have gone through a similar level of Identity proofing, and either be in an interoperable format or easily cleaned and converted to these states. Although this strategy may efficiently provide an initial set of identities of the stock of people in the country—by virtue of the fact that it can be done without contact with the population—it may require

additional data collection, which can be done either through an active mass registration campaign and/or by collecting this data when people visit registration points to replace lost, damaged or expired smartcards or to update certain attributes (e.g., as in **South Africa** and **Viet Nam**, which are upgrading their paper-based national ID systems in this manner). If this approach is adopted, then it must comply with relevant laws, regulations, and good practices related data protection—e.g., related to purpose specification, data sharing, etc.—and the legal frameworks that govern the source registries and databases and the new ID system. For example, the data might not be able to be migrated from other registries and databases unless people provide explicit consent.

- **Passive and/or active mass registration.** A country may need or want to collect new data for the ID system. This can be done through a “mass registration” exercise, either **passively** (i.e., people visit a permanent or temporary registration point when they need or want to) and/or **actively** (i.e., mobilizing teams to travel across the country to register communities, similar to a population and housing census but not necessarily visiting individual homes). Passive and active approaches are not mutually-exclusive, and importantly should not be combined with a statistical census (see Box 32).
 - A **passive** approach can be easier to manage than active registration. However, unless there are sufficient incentives for the population to enroll, it can take longer to reach the level of coverage necessary for certain use cases or benefits (e.g., as in **India**, where cash transfer recipients were obliged to register with Aadhaar to continue receiving benefits, and then civil servants to continue receiving a salary). If demand is high, then the capacity at certain registration points can be increased or decreased as needed.
 - An **active** approach typically involves a large mobilization of resources and personnel—provided by the government or the private sector—along with information campaigns and intense outreach in coordination with local governments and local media to cover large portions of the population according to a defined schedule. Active mass registration campaigns are typically rolled out *geographically*, moving sequentially through the territory (e.g., as in **Rwanda** and **Malawi**).

Box 32. The relationship between mass registration and population (statistical) censuses

A population and housing censuses enumeration should not be combined with the mass registration for a foundational ID system. While it may seem that the exercises are similar in the sense that they both intend to collect data on the entire (or close to the entire) population and that there are potential efficiency gains by doing them together, they are very different exercises and integrating them will undermine both important exercises. However, a population and housing census is an effective method of *measuring* the coverage of a foundational ID system and identifying any correlation between under-coverage and certain characteristics—e.g., socio-economic status, ethnicity, and location.

The purpose of a population and housing census is to produce a wide range of data that provides a snapshot of the resident population by demographic attributes, socioeconomic profiles and geographic location—i.e., it collects significantly more information than what is recommended for a foundational ID system. Furthermore, international standards and recommendations regarding data protection and statistics—including the Fundamental Principles of Official Statistics (<https://unstats.un.org/unsd/dnss/gp/fundprinciples.aspx>)—call for individual-level data collected for statistical purposes to be kept confidential and for this data to be used *exclusively for statistical purposes* because respondents are more likely to provide accurate and comprehensive information if they are not individually identified. Conversely, the purpose of a mass registration is to individually identify people and to collect as minimal data as possible.

Approach to continuous registration and data updates

Once the initial phase has been completed—or for existing ID systems, once upgrades are completed—a “steady-state” approach to registration requires a strategy for the **continuous updating** of existing identity records and **continuous registration** of the flow of new people enrolling for the first time. Without a plan for continuous updating, ID systems and records will become out of date, necessitating repeated—and costly—ad hoc data collection exercises. This updating process is typically done through:

- **“On-demand” registration and updating.** Following a mass registration campaign and/or building on existing databases, on-demand registration mechanisms are typically used to (1) incorporate the “flow” of additional enrollees (i.e., for new births, migrants, and people who were not initially registered), and (2) update existing records or collect supplementary data. This typically requires people initiating updates or additional enrollments themselves and may involve the same or different procedures and infrastructure as mass registration campaigns (e.g., mobile campaigns and/or dedicated enrollment centers).
- **Links with other databases—particularly with the country’s civil registration system.** In addition to registering new people and making updates to existing records through on-demand registration, linkages with other data sources can help keep identity records up-to-date. Most importantly, this includes automated notifications from the civil registration system when a person has died, allowing the identity provider to disable or retire the identity. It may also include notifications of new births from the civil registration system to generate an identity (if birth registration is linked to the ID system generation), notifications of new legal residents from an immigration database, and more.

Countries should ideally combine the delivery of ID and civil registration systems’ services into one physical point and with ‘one stop shops’ where they exist, rather than set up new frontline

service delivery points. Foundational ID and civil registration systems are the core identity services in a country and it therefore makes sense for their frontline services to be integrated. As was demonstrated through *ID4D's research on cost drivers of ID systems*, sharing physical infrastructure and human resources between foundational ID and civil registration systems can significantly reduce capital and operating costs.

In addition to these processes, it may be necessary to hold **periodic targeted outreach campaigns** to communities where the initial coverage of the system was low, and/or where people find it difficult to complete on-demand registration or updating procedures. For instance, **Malaysia's** National Registration Department and **Peru's** RENIEC periodically travel to remote communities in coordination with local government. Likewise, it will be necessary to make **home visits** to provide registration and data updating services for elderly, people with disabilities, and institutionalized persons who cannot physically travel to registration points. Social welfare agencies and local government often work with ID agencies to identify such vulnerable persons. For example, **Thailand's** Bureau of Registration Administration has registration teams in all 76 provinces who work with district governments to schedule visits to the homes of people who cannot get to district offices, including hospitals and prisons.

Insourcing and outsourcing registration

Countries can choose to insource and/or outsource mass and continuous registration and data updating for the ID system, depending on their capacity, budget, timeline, and the availability of outsourcing partners—e.g., other government agencies at different levels and the private sector (see Table 30). For example, given the complexity of planning and managing a mass registration drive and the human resources and hardware required over a sustained period, practitioners may choose to outsource the initial mass registration, while transitioning to insourcing continuous registration and data updating as they move to steady state, or they may insource registration for populations where there might be insufficient commercial incentive for outsourced registration agents to cover—e.g., smaller rural or remote communities—while urban and densely populated areas are covered by outsourced partners.

India has outsourced the majority of its Aadhaar mass and continuous registration and data updating activities to a wide range of public and private sector “enrollment agents” that are empaneled through a procurement process. The incentives of being paid for each successful registration and competition between the enrollment agents has helped Aadhaar scale up quickly. However, the UIDAI maintains strict supervision over the registration and data updating operations, including certifying equipment, providing the registration software client, and installing an operating system on registration devices that allows UIDAI to monitor the device's use at the level of keystrokes. Meanwhile, **Malawi** and **Uganda** completely insourced their mass registration and continuous registration and data updating, with both countries also completing their initial mass registration relatively quickly because of the strong link with use cases and well-planned registration operations.

Table 30. Insourcing and Outsourcing Registration

Type	Description	Advantages	Disadvantages
Insource	<p>The ID authority procures its own registration equipment, hires and trains its own registration staff (temporary or permanent), develops its own registration plans, manages its own logistics (travel, security, installation), and/or provides its own technical support.</p> <p><i>Some of these functions could also be outsourced.</i></p>	The ID authority retains full control and accountability for the implementation of registration and it is easier to change plans (compared to renegotiating an outsourcing contract).	<p>The ID authority must have substantial capacity to carry out procurements, manage human resources and equipment, and to coordinate logistics, and, without proper planning, Government procurement requirements may make operations less flexible.</p> <p>After a mass registration, the ID authority will have to find a way to repurpose the surplus registration equipment.</p>
Outsource	<p>The ID authority hires the services of one or more public and/or private sector organizations as registration agents to carry out all the same operations described above, and they are compensated based on each successful—i.e., unique—registration.</p> <p>The ID authority will likely still have to provide registration software, carry out supervision and monitoring, certify that equipment meets relevant standards, and lead outreach and awareness raising.</p>	<p>Particularly during an initial mass registration, outsourcing allows an ID authority to transfer complicated operations to other actors, which frees up their resources to focus on other core functions. Competition among registration agents can also create incentives for them to innovate and to register the population quickly. Furthermore, by creating an ecosystem of registration agents, there is a possibility that the cost of equipment will be driven down through the competition among hardware providers.</p> <p>Outsourcing to other Government agencies—e.g., social security and health insurance agencies—can also leverage their offices and use the opportunity of when people use their services to simultaneously register.</p>	<p>Unless the ID agency has visibility on operations and management, there are risks of poor data quality and performance because of the financial incentive to register as many people as quickly as possible, as well as data protection and privacy risks—e.g., that personal data is retained by the registration agent—and whether or not agents will adhere to stated policies (e.g., regarding fee charging or identity evidence).</p>

Generating demand through awareness raising and incentives

While the above sections deal with the *supply* of registration and data update services, **generating demand is equally—if not more—important.** Without demand, the best registration strategy will be ineffective. The public need as few barriers as possible and sufficient reasons to travel to a registration point and to potentially queue for hours before not even receiving their ID credentials (in cases where Identity proofing processes delay issuing). This demand can be generated through effective communications and by linking the ID system with the delivery of services.

While *Section III. Public Engagement* provides general guidance regarding communications, there are several additional lessons specifically for mass registration:

- **Describe the process and requirements clearly.** People should be able to easily understand what they need to do and bring to register and/or update data. The information should be circulated through all potential channels—e.g., radio, television, print media, flyers, posters and through local government—and use accessible language. The use of images and graphics will also help low literacy populations.
- **Set up a call center and use social media to engage with the population.** The public will inevitably have questions and may need to report complaints. A toll-free hotline and social media pages should be made available to the public, with the ability to scale this up or down depending on forecasted demand. While complaints can be accepted through these channels, they should be dealt with through the grievance redress mechanisms.
- **Manage expectations.** The introduction of an ID system can create excitement among the population, particularly if the country may not have strong existing foundational systems. The news media and the public—e.g., through social media—will want to know when registration will be made available to them and when they will receive credentials. Since the initial mass registration is a moment when trust and confidence in the ID system can be won or lost, announcing unrealistic targets is likely to negatively affect the reputation of the ID agency and the foundational ID system. Conversely, early completion announced timelines can create a positive reputation. Practitioners should therefore be careful to only announce targets that it is certain of meeting them.
- **Promote positive reasons to register.** As with any communications for behavioral change, awareness raising should be informed by insights from the population through market and end-user research. Such public consultations should help identify the most compelling reasons that people would want to register—e.g., to receive an ID card, because of national pride, or the expectation that it will be easier to access services such as banking and e-government. These positive messages can help mobilize the population to spend their time to participate in a mass registration exercise. On the other hand, describing negative consequences of *not registering*—e.g., that people may not be considered a “good citizen” or that they could have “something to hide”—could create suspicions about the motives of the ID system and have the reverse effect of discouraging the population to register.
- **Coordinate with local government and other authorities.** ID authorities should work closely with provincial and local governments and other trusted government bodies—e.g., social

welfare agencies—to get their help in raising awareness about the importance of registering and how to do so. Local governments and local leaders in particular can help to mobilize the population when registration teams visit a community by promoting the visit a few days and weeks in advance.

- **Prepare for crisis response communications.** Considering the large and complex nature of these operation, it is very possible that problems will emerge during any initial mass registration. Real examples of problems that ID systems have encountered include people being denied registration because of a misunderstanding of procedures by registration staff, people standing in a queue fainting because of heat, and allegations that registration staff are requesting bribes. While steps can be taken to reduce these and other problems, they are likely to be reported on news or social media if they occur. The ID authority should therefore be ready to publicly respond to these incidents effectively and with empathy.

While linking the introduction of an ID system to accessing certain services will create an incentive for people to register, people should not be denied essential services because they have not registered—whether by choice or not. Especially early in implementation, certain segments of the population will not have been able to register in the ID system. Therefore, instead of making services contingent on possession of a specific credential or authentication through a particular ID system, people should still be allowed to access these services using credible alternative IDs and methods of authentication. The use of the new ID could also be turned into a positive incentive—e.g., express lines in government offices or reduced fees such as for passport and driving license applications. If an ID system is going to be a requirement for a service—e.g., a cash transfer or subsidy from Government—then there should be a reasonable transition period and mechanisms for beneficiaries to register.

Registration operations

The registration and data update processes must as easy and simple as possible. Most people should be able to complete the data collection process in less than five or ten minutes after waiting in a queue for as little time as possible. The overall experience should be a positive one, whether registration is done at temporary or permanent registration points.

Key lessons for designing registration processes

Based on the experiences of a wide-variety of countries with different contexts and ID systems, the following good practices have emerged regarding registration operations overall:

- **Inclusive and flexible evidence requirements.** As described in [Section III. Registration & Coverage > Proving Identity Claims](#), having strict requirements for the documentation that people provide as evidence of their identity is not only likely to exclude some populations but also increase the cost of registration because people may have to obtain those documents if they do not currently have them.
- **Operating times should account for people's regular lives.** Registration points should be open outside of traditional work hours—e.g., 7am to 7pm—and on weekends to allow people who work during regular business hours to register without taking time from work. During

business hours, it could be useful to have registration teams to visit workplaces with large numbers of people

- **Provide appropriate space and facilities for large crowds.** When people visit temporary or permanent registration points, there should be sufficient space and seating—with prioritization given to less mobile persons—and the conditions should allow people to wait as comfortably as possible—e.g., with lighting, air conditioning or fans, shade (if outside), toilets, enough waste bins, and food and drinks available nearby. If it is a temporary registration point, registration staff should ensure that waste is not left behind when the registration teams move to their next location.
- **Crowd control and physical accessibility are very important.** There should be an adequate number of staff who can greet people and manage the queue, as well as equipment—e.g., signage and rope lines or other barriers. Registration staff should also coordinate with local police and medical personnel who can respond in case there is any incident. If there are security challenges, it may be necessary to request police to stay at the registration point or hire temporary security guards. Whether temporary or permanent, registration points should be reasonably accessible by public or private transport, as well as being accessible for persons with physical disabilities—e.g., with ramps and elevators.
- **Leverage existing physical spaces and infrastructure where possible.** Schools, local halls and sports facilities can provide excellent physical infrastructure for an initial mass registration—they are typically accessible, safe, and have sufficient space. These are also often spaces used by Government and civil society to convene local populations and are therefore familiar to the population. ID agencies should work closely with local governments and election bodies to identify suitable sites since they respectively have experience with organizing community events and setting up temporary polling stations across the country.
- **There should be exception handling mechanisms built into the process and software, particularly for people who cannot provide biometrics of adequate quality.** Some people—e.g., manual laborers, the elderly, persons with disabilities, diabetics, etc.—will be unable to provide fingerprints or other biometrics of a quality that would be acceptable for the ID system. In order to not prevent them from gaining access to the ID system, there should be exception handling mechanisms that allow a registration staff or their supervisor to override the requirement for certain biometrics.
- **Registration staff should authenticate themselves at the beginning and end of collecting data on each applicant.** To facilitate auditability and ensure accountability for each and every identity record, the registration staff should authenticate themselves with a high level of assurance at the beginning and the end of each applicant's registration.
- **Encrypt data on registration devices and reduce the amount of time that personal data is stored on them.** Each registration packet comprises sensitive data that if breached could have significant consequences for the concerned individual. While it should be possible to edit data during the process of the data being collected—e.g., for the applicant to verify the data themselves and to correct mistakes if needed—the data should be encrypted the moment the data collection is completed and should only be able to be decrypted by the central systems that are doing the identity proofing. Furthermore, the data should be

immediately uploaded to the central server and then wiped from the local device to reduce the risk of the data being lost if the physical device is lost, stolen or damaged.

- **Provide people with a registration receipt as a reference.** If Identity proofing and deduplication is not going to be completed on the spot, then people should be provided with a receipt containing a temporary reference number for their registration, so they can follow up on the status of their registration—e.g., through a web portal, call center, app or USSD—or potentially update their data before the identity proofing has been completed. The receipt could be printed using a regular desktop printer or a high-quality thermal printer, which could be shared among several registration devices. It is critical that the receipt is durable and contains the data that was provided at the time of registration, so the applicant can easily refer to the data they provided.
- **Allow people to update information provided after they have registered and before the identity proofing and deduplication process has been completed.** In some cases, people may need to update certain attributes—e.g., address and phone number, or possibly even date of birth if they have found additional evidence—after they have been through the initial registration but before the identity proofing process has been completed. This can be facilitated using the registration receipt that was provided after the initial registration and by uploading an amended “packet” of data to the central queue and attaching that to the original registration packet.
- **Pre-registration and scheduling appointments can save time.** By allowing people to submit data and supporting documents in advance—e.g., through a web portal, with the data retrieved at the registration point using a reference number and/or barcode—and/or to schedule an appointment to have the data validated and biometrics provided can substantially reduce queues and increase convenience for the population. However, this will not necessarily help populations who have lower levels of literacy and/or no access to the internet, but such services could potentially be facilitated for these populations by local governments and civil society.
- **Express queues for people with special needs.** It may be expedient for the broader exercise to provide an express lane for families with children, the elderly, people with a disability, and any other persons with special needs, if there is sufficient demand from these populations.

Hardware and Equipment

The equipment required for carrying out registration will depend on the data being collected and the anticipated environmental conditions at registration points. At a minimum, a registration kit will comprise a computer, laptop, tablet or smartphone, and then with data capture devices—e.g., camera, fingerprint scanner and iris scanner—either integrated into the device, integrated into a case or connected via cables peripherally. If the kit is going to upload registrations live, then it will need to have a reliable network connection. Additional accessories such as a plain color backdrop and lighting (for facial images), a second screen (for the applicant to see the data as it is being entered), a printer (for producing registration receipts), scanners (for scanning supporting documents), and power sources (as backup or for running the registration kit in areas without electricity) may also be required. It is critical that registration equipment is durable for the conditions where they will be

deployed—e.g., resistant to water and dust—and that they come with appropriate warranties, performance guarantees, and technical support.

The functional and technical design of the ID system should dictate the requirements for the registration equipment (and not vice versa), including the standards to be adopted. For example, if ten fingerprints are going to be collected then using a single or dual fingerprint capture device might require an ABIS that is permutation invariant because the fingerprints could be captured in any order, unlike a slap scanner, which captures fingerprints in groups of four, four and two). Likewise, it is important that the biometric capture equipment can capture raw images of appropriate quality and in open standard formats—e.g., the fingerprint scanner should be able to capture 500dpi images in WSQ or JPEG2000 format.

A key decision that has to be made is whether to choose registration tablets and smartphones and/or laptops/desktop computers (and, if laptop, whether the whole kit is integrated into a case or not). The use of tablets and smartphones has substantial benefits in terms of durability, mobility, reduced cost (compared to a laptop or desktop computer), and potentially longer battery life (depending on what devices are integrated into or connected to it). While biometric capture devices can be connected by cable or Bluetooth to tablets and smartphones, a growing number of these devices are entering the market with integrated fingerprint and iris capture devices, including some that have a fingerprint slap scanner rather than single or dual fingerprint capture devices. Laptops and desktop computers have an advantage in terms of having a larger screen, being able to run Windows operating system, being able to connect more devices, and having more commodity hardware options. The integration of all the devices into a tablet, smartphone or, for laptops, a case, reduces the number of “loose” equipment that could be lost, damaged or stolen, and a sturdy enclosure can also help the equipment withstand bumps, drops, water, and dust. However, integrating devices may also substantially increase the cost because fewer suppliers offer such products. Finally, while cases are convenient to set up at registration points and best protect equipment against the elements, they can take up a lot of desk space and can be heavy and bulky when moving around. Practitioners should carefully consider the technical and functional requirements—including the contexts where registration will be taking place—in order to make an informed decision with respect to the form factor(s) of registration kits.

Considering emerging innovations, procurement of registration equipment should—to the maximum extent possible—be based on functional requirements and standards rather than technical specifications. Generally, it is good practice for procurement documentation to describe functional requirements and standards rather than technical specifications to allow the market and potential bidders to develop innovative solutions to meet those requirements. For example, specifying “a DSLR camera” rather than “a camera that can produce facial images that meet *ICAO Doc 9303* standards” would eliminate potentially much cheaper high definition webcams or cameras integrated into tablets and smartphones, even though they would meet the same requirement.

Registration equipment procured for an initial mass registration should be procured with a view to how they can be repurposed when demand for registration reduces. A large number of registration kits will need to be procured if a country intends to reach high levels of coverage more quickly. Once a mass registration is winding down and an ID system is reaching steady-state mode, there is an opportunity to use the surplus equipment for various purposes—e.g., using fingerprint capture devices or biometric registration tablets for authentication at points of service delivery.

Human Resources

One of the most challenging aspects of an initial mass registration is hiring, training and managing a large number of—often temporary—staff. When insourcing registration, the ID authority will need to deal with these challenges directly; when outsourcing registration, they will need to ensure that partners have sufficient capacity to do the same.

For estimating staffing numbers, each kit will need at least one staff member and—if the kits are to be operational for more than five days a week—there needs to be additional staff who will rotate. In addition, there will need to be supervisors—e.g., one per five to ten registration staff—and other staff potentially for security and crowd control.

The staff doing the actual data collection will need to have strong digital literacy and communication skills and will need substantial training on the use of the registration software and hardware and on what to do if something goes wrong—e.g., exception handling for people who cannot provide biometrics. It is good practice for training to be “live” through which the staff will practice registration of real persons and how to deal with different scenarios—e.g., when the software crashes, when fingerprints or other biometrics of adequate quality cannot be captured, and when someone does not have certain documents. Furthermore, there should be comprehensive manuals produced and provided to registration staff and supervisors.

The initial mass registration drive is an opportunity to hire and build the skills of young people. With youth unemployment rates in many countries significantly higher than the rest of the population, prioritizing them to take data collection positions can have a range of broader social and economic benefits. By providing practical experience and formal employment and developing skills in how to operate and maintain software and hardware, their employability could markedly improve. Moreover, they could potentially transition to permanent staff in an ID authority as they become familiar with the system. **Malawi** is an example of a country that has done this by partnering with local universities to recruit students.

When doing a geographic-based initial mass registration, it can be advantageous to hire registration staff locally. Hiring local staff—e.g., within the same region or province—can reduce travel costs but can also help if there are local languages, dialects or cultural considerations.

Proofing identity claims

Once identity data has been collected through the registration process—i.e., people have “claimed” a particular identity by completing an application and providing supporting evidence—it must be “proofed” in order to determine its veracity. Identity proofing enables the ID provider to:

- Resolve a claimed identity to a single, unique identity within the context of the population
- Validate that all supplied evidence is correct and genuine (that is, not counterfeit or misappropriated)
- Validate that the claimed identity exists in the real world
- Verify that the claimed identity is associated with the real person supplying the identity evidence (*NIST 800-63A:2017*)

The identity proofing process is fundamental to ensuring the accuracy and trustworthiness of the identities created. In addition, the requirements for identity proofing have important implications for how convenient and resource-intensive the registration process is, which in turn affects both the inclusivity and cost of the program. This section focuses on relevant choices regarding fundamental processes of the identity proofing phase of registration:

- **Validation.** Checking the validity, authenticity, and accuracy of the supporting documents or evidence provided and confirming that the identity data is valid, current, and related to a real-life person.
- **Deduplication.** Using biometric recognition (using biometric identification to identify other identities already registered that could be a match) and/or demographic deduplication algorithms—e.g., fuzzy logic—to ensure that a person is unique before they are enrolled.

Figure 24. Key considerations for identity proofing

Inclusion	Reliability	Sustainability
Marginalized groups may not always have supporting documentation to prove their identity, and complex registration and proofing requirements may present financial and logistical barriers	The strength of the deduplication and validation processes will determine the accuracy and uniqueness of identities and contribute to the level of assurance for transactions	Extensive identity proofing requirements will add time and expense to the registration process

Validation

Validation creates confidence that the identity information contained about a person in the ID system reflects who they really are. By determining the authenticity, validity, and accuracy of the identity information the applicant has provided on the application, the identity provider can be reasonably sure that the identity is “real” and “correct.” Robust validation may require a variety of processes involving several types of evidence, investigative measures, and technologies, as shown in Table 31.

Table 31. Example measures and technologies used in identity validation

Measure	Description	Potential Requirements
Requiring supporting documents	Applicant presents one or more acceptable documents, such as birth certificates, passports, driver’s licenses, voter IDs, property titles, tax ID, ration cards, school ID, utility bills, etc.	<ul style="list-style-type: none"> ▪ Document scanners ▪ Document readers with automated fraud detection systems (docometrics) ▪ Forensic analysis

Measure	Description	Potential Requirements
Verification/ validation against external sources	Validation of the applicant's identity and/or the validity of supporting documents by checking against other databases and systems, such as the civil register, social security records, local community records, etc.	<ul style="list-style-type: none"> Digitized civil register (or other relevant systems against which the identity will be verified) Secure access portal for data queries maintained by the organizations that own the external data Access privileges for the ID provider
Community witnesses or affidavits	Testimonials from trusted community members or organizations who can act as a witness—either in person or in writing—to the existence of a person and/or specific attributes (e.g., village of birth)	<ul style="list-style-type: none"> Affidavit forms (paper or online) Oral interviews Increasingly, access to social media with vetting from friends
Digital footprints	Increasingly, people leave behind a digital trail or “footprint” based on their transactions and interactions, which can potentially be used as evidence for a person's identity. To our knowledge, however, this method has not been used for a foundational ID system and would require a serious data protection impact assessment.	<ul style="list-style-type: none"> Software that creates a body of knowledge around an identity Potential “challenge-response” proofs of identity where a person is asked a question extracted from their footprint that only they are likely be able to answer correctly

Source: Adapted from the *Digital Identity Toolkit*

Ideally, all persons should be documented in the civil registration system at birth or upon entry into the country, providing an authoritative source of identity information and documents.

Unfortunately, this is not the case in many countries, where many people often lack basic documents—e.g., birth certificates, passports, utility bills, driving licenses, etc.—to validate or verify their identity at the time of registration. Refugees and migrants who were not born in the country where they reside will not—by definition—be included in the country's civil register. Many vulnerable people—particularly poor, rural, and slum dwellers—may also not have formal addresses or a reliable proof of their location of residence. Even if people do have some form of documentation, it may not be trustworthy if these documents are easy to forge or counterfeit.

In such cases, countries have developed alternate mechanisms to ensure that registration in foundational ID systems is inclusive, including the following (see Box 33):

- **Accepting a wide variety of supporting documents:** If a certain document—e.g., a birth certificate or voter card—does not have universal coverage within the population, it should not be the *only* acceptable proof of identity for the registration process. Instead, countries can allow for substantiating documents from a variety of sources (e.g., **Peru**, **India**, **UK Verify**). In **Malawi**, different documents were given different reliability “scores,” and applicants for the national ID could provide various combinations of documents to reach the required threshold (see *Malik 2018*).
- **Decoupling nationality from identity:** Providing proof of nationality is often one of the most arduous documentation requirements for ID systems, particularly in countries with *jus*

sanguinis nationality laws (see ID4D's *The State of Identification Systems in Africa* for some examples). Where the goal of an ID system is primarily to facilitate service delivery and online authentication for all people within the territory, nationality may not be directly relevant. In **India**, this choice significantly simplified registration timelines, reduced costs, and helped with the rapid uptake of the Aadhaar system.

- **Using reliable people to vouch for a person's identity:** Certain countries use an “introducer” or “witness” who can verify the applicant's identity or particular attributes (e.g., residence or birth in a particular village). In **India**, for example, people without supporting documents can rely on a pre-registered introducer to assert their identity, and applicants who can demonstrate that they are the head of household can effectively serve as “introducers” for their family members. This model, however, requires that introducers frequently travel to registration centers, which may not always be feasible if they have full-time jobs. Furthermore, to ensure inclusivity, introducers must be available to all, and particularly to the vulnerable and marginalized groups that are most likely to need them.

A combination of the above strategies could also be used to allow for identity proofing at different levels of assurance (see *Section III. Standards*).

Box 33. Examples of inclusive identity proofing processes

India's Aadhaar system aimed for an inclusive and risk-based approach to registration to maximize the coverage and utility of the system while minimizing costs. Importantly—because Aadhaar does not provide legal proof of nationality—**no documentation of nationality** was required. In addition, low birth registration rates meant that enrollment agents were allowed to **accept any of 18 documents for proof of identity**, 34 documents for proof of address, and 9 for proof of date of Birth. (For a list of acceptable documents, see https://uidai.gov.in/images/commndoc/valid_documents_list.pdf).

In addition, people without any supporting can use **approved introducers to attest to their identity**. This includes people with high credibility, and particularly those who work with vulnerable groups (e.g., social workers, employees of the Registrar, postal workers, teachers, hospital staff, local government officials, etc.). The accountability of the introducers is achieved through an approval process by UIDAI agents (Registrars), a central registry of introducers that records who they have introduced, and punishments for false assertions. (See page 29 of https://uidai.gov.in/images/regulation_1_to_5_15092016.pdf for UIDAI's regulations on introducers). In addition, those without documentation were able to get **signed letters from Gazetted Officers** (e.g., a senior official in the local government) with the applicant's photo, their details, and the official letterhead and signature/thumbprint of the Officer.

Although there were initial concerns about applicants submitting incorrect or fake names for Aadhaar, this has not been a significant issue. Although accepting many types of documents has facilitated inclusion, a large portion of the population (particularly the wealthy and middle class) has applied using passports, driving licenses, and other trusted documents. For many poor people, Aadhaar has been their first reliable form of identification and a source of pride, creating incentives to provide correct information. In addition, the Government widely disseminated the consequences of providing false information, such as accessing services with providers where they had previously registered under a different name as well as fines and potential imprisonment.

Crucially, the reliability of the Aadhaar system and its ability to provide a high level of assurance is achieved through **biometric deduplication** to ensure that each person can only register once. Thus, even if they gave a false name, they are only able to register once, and can be authenticated as the same person over time.

Malawi has an extremely low level of birth registration. However, the country used a different approach to verification for the national ID card because it also provides legal proof of nationality. Malawi assessed the quality of existing IDs and created a points-based system, whereby different supporting documents or an affidavit of a local chief were given a score based on how trusted they could be for *both* identity and nationality. Even for those who could not meet the threshold there were administrative mechanisms to process their claim to an identity. For more information, see pp. 24-36 of *Malik (2018)*.

Peru began its national ID (DNI) system requiring birth certificates for registration, however it experienced high rates of exclusion among vulnerable populations. After the initial rollout, Peru had targeted campaigns that authorized municipalities and Civil Registry and Electoral Offices to accept applications and reapplications from vulnerable populations with minimum requirements (e.g. witnesses of birth, doctor's or midwife's note, baptismal certificate, etc.).

On the whole, the validation process can be costly, as it involves the collection—and typically scanning—of evidence, as well as its subsequent examination and validation through mechanisms that could include cross-referencing against external databases (birth or death registers, health records, etc.), forensic examination of documents to ensure they are not forged, and interviews with individuals and members of the community. The more data that needs to be validated (and the more robust the validation procedures are), the more expensive the exercise will be.

Thus, it is important to adopt a detailed policy on what constitutes acceptable vetting within a framework of risk tolerance. This should represent the shared vision of multiple stakeholders—including the community—as to how to best prove someone's identity and the required levels of assurance for different use cases.

Deduplication

Once identity information is validated and enrolled, identity proofing typically continues with deduplication to ensure that each applicant is unique in the database. In the abstract, deduplication involves comparing a subset of the applicant's data—e.g., core attributes and/or biometric templates—against all previously enrolled records (i.e., a 1:N or N:N matching process) to determine whether there is a match.

If no match is found, the identity is considered new or “unique” and is passed on to the next phase (e.g., registering the person and assigning them a unique number). If, on the other hand, a match is found, it means that this person may have previously enrolled. An **adjudication process is then performed by a trained operator** to validate whether the computer-identified match is an error (a false-match) or a genuine duplicate (i.e., the person has already enrolled). This type of deduplication process helps ensure the uniqueness of each record in the database.

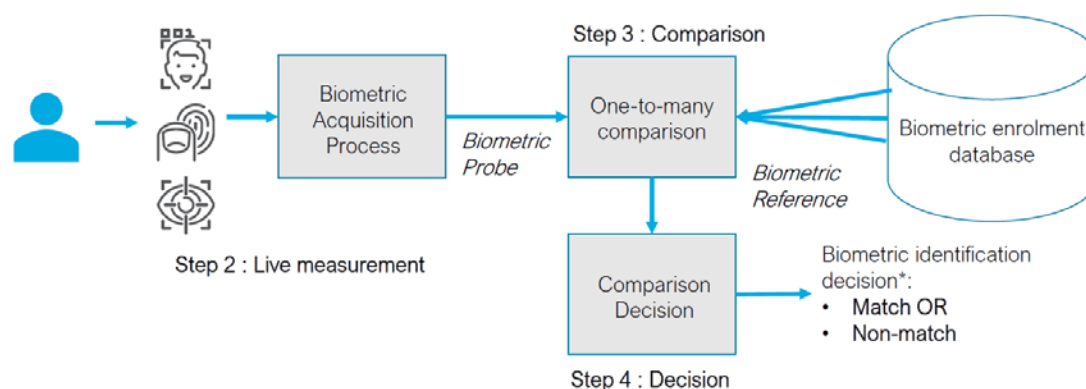
Currently, biometric recognition is the most accurate technology for deduplicating identities, particularly in large countries where many people many share similar biographic attributes. This process uses a search engine called an Automated Biometric Identification System (ABIS)—or an Automated Fingerprint Identification System (AFIS) if using only fingerprints—to perform duplicate biometric enrollment checks of each new applicant (see Figure 25). The AFIS/ABIS is a complex and computationally intensive system that requires in-depth knowledge of biometric systems, IT systems,

cybersecurity, and operations. Note, however, that biometric deduplication is rarely 100 percent automated and, in some cases, requires manual adjudication or verification by a human operator.

However, while biometric recognition may be the most advanced technology available for deduplication, it may not always be desirable, given the cost of the technology, potential issues related to inclusion, and data protection concerns discussed in [Section III. Data > Biometric Data](#).

For more technical guidance on the use of biometrics for deduplication, consult the ID4D Biometrics Guide (*forthcoming*).

Figure 25. Example deduplication process using biometrics



Source: ID4D Biometrics Guide (*forthcoming*).

CREDENTIALS & AUTHENTICATION

The credentials and authentication mechanisms adopted by the ID system dictate how the system will be used by people in their daily lives. As such, they are central to the experience that end-users and relying parties have when they interact with the system, the level of assurance it provides for transactions, and much of its functionality and usage. In addition, the types of credentials and authentication mechanisms adopted play a large part in determining the overall cost of the system. Countries should therefore strive to provide credentials and authentication mechanisms that can provide a high enough level of assurance while being context appropriate.







This section focuses on different technical options related to:

- Common types of physical and digital credentials issued, including ID numbers, cards and mobile ID
- The process for issuing and collecting cards (or other physical credentials)
- Authentication mechanisms for offline/local and online/remote authentication, as well as federation arrangements that allow an entity to accept credentials issued by third-party identity providers for authentication and authorization
- Levels of assurance for authentication based on identity proofing, credentials, and authentication mechanisms

For more details on emerging technology for credentials and authentication, see the *ID4D Technology Landscape report*.

Figure 26. Key considerations for credentials and authentication

 Inclusion	 Reliability	 Data Protection	 Sustainability
Certain credentials and authentication mechanisms may pose accessibility challenges for particular groups, including illiterate people and those with limited internet or mobile phone access	The form and format of credentials—including security features—and authentication mechanisms used contribute to the level of assurance the ID system provides for transactions	Credential formats—e.g., number structures and information printed on a card —and authentication protocols should be privacy enhancing (e.g., using yes/no responses whenever possible to protect personal data)	Credentials are a significant contributor to the cost of an ID system, ranging from an estimated 10-40% of total costs depending on the form factor

Types of credentials and authenticators

A credential can be defined as any document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Simply put, a credential is the thing that a person presents—in person or remotely—to say “this is who I am.” The types of credentials issued in an ID system vary along multiple dimensions, including whether or not they are physical (i.e., they must be physically carried by a person in order to use them), and whether or not they are digital (i.e., they are machine readable and therefore can be used in a digital environment). In addition to credentials themselves, the authentication process may involve presenting the credential along with additional factors (i.e., “authenticators”) that bind the person to the credential, offering assurance that the person in possession of the credential is its rightful owner. Common types of credentials and authenticators are shown in Figure 27.

Figure 27. Examples of credentials and authenticators commonly issued by foundational ID systems



Credentials vary in terms of format and functionality—e.g., the medium in which identity data are stored and their ability to be used for authentication in multiple environments—as well as the levels of security they provide and their cost. Historically, most countries have used physical documents such as national ID cards and birth certificates as the basis for their foundational ID systems. Advances in digital technology have led to the digitization of physical credentials that now include magstripes, barcodes, and/or chips that allow them to be used in a digital environment.

As societies become more digital, we have begun to see a move toward digital-only ID systems that do not rely on the possession of a physical credential. Such approaches use credentials that are stored only on computers, mobile devices, and servers—or in the form of user names and ID numbers—and which rely on biometrics and other factors for authentication. In the **UK**, for example—where people already have a variety of physical documents to prove who they are for in-person transactions—the GOV.UK Verify system provides digital-only ID credentials that allow end-users to authenticate themselves remotely via multiple factors (e.g., a username and password + mobile authenticator) for online services. The BankID systems in **Sweden** and **Norway** provide similar “layers” of digital authentication for e-services that do not rely on physical credentials.

However, there are certain limitations to the use of digital-only approach to credentials and authentication. In **India**, for example, the Aadhaar system allows people to authenticate themselves for in-person and remote transactions with only their unique ID number (called “UID”) and a fingerprint or one-time password (OTP). However, authentication through this method—i.e., with no physical credential—requires connectivity to a database, which may not be feasible in countries with

unreliable or uneven internet or mobile coverage, although these gaps are narrowing over time. In addition to the connectivity concern, experience suggests that in many contexts, people may prefer physical credentials as they are more intuitive or easier to use and/or hold a symbolic value. In India, for example, many people still carry the Aadhaar “card” (a paper receipt with UID printed on it) in order to avoid remembering the 12-digit number (*IDinsight 2018*). The viability of the ID-number-as-credential option therefore requires careful consideration of the country context and public consultations to better understand people’s preferences.

As with other topics discussed in this Guide, **the choice of credentials should be based on multi-stakeholder consultations and user-centric design considerations that reflect the overall vision and use-cases for the ID system, as well as costs and other context-based constraints.** For example, areas with low-connectivity and high levels of fraud may require physical credentials that can be securely authenticated in an offline-environment. Where internet connectivity and/or mobile phones are widespread, virtual credentials may be more feasible as a primary tool for authentication.

Ideally, the ID system should allow for easy adoption of multiple credential technologies, including new technologies that may emerge in the future. Through the use of open standards and procurement practices that avoid vendor and technology lock-in, practitioners can ensure that the system is able to adapt and take advantage of new solutions. In addition, a number of ID systems issue multiple types of (optional) credentials, as discussed in Box 34. Giving people choice over their credentials will increase convenience and nurture innovation around ID services.

Box 34. Examples of multiple types of credentials in one country

ID credentials may take **multiple forms** within a single country. In **Austria**, for example, the national ID can be issued as a physical “citizen card” (*Bürgerkarte*) or a virtual mobile ID (*Handy-Signatur*). Both can be used for digital authentication and e-signatures. For more information, see <https://www.buergerkarte.at/en/>.

In **Estonia**, people with the standard national ID smartcard (ID-card) can also apply for a supplementary smartcard called “Digi-ID,” which provides the same functionality (digital authentication and e-signatures) but does not include a photo of the person and therefore is intended only for non-face-to-face transactions. Estonia also offers two types of mobile ID for digital authentication, e-signatures and access to online services: one, called “Mobiil-ID”, leverages PKI-based SIM technology and is offered by Estonian mobile companies; the other, called “Smart-ID”, is an app that can be downloaded on any smartphone. For more information, see <https://www.id.ee/>.

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)*.

The remainder of this section focuses on important issues related to three of the most common types of credentials used in foundational ID systems: ID numbers, cards, and mobile IDs.

Unique ID Numbers

In any ID system, identifying numbers—including unique ID numbers (UINs), also sometimes known as national ID numbers (NINs)—are the most basic type of identifier. They are issued automatically when a person enrolls, and their default function is to serve as a record locator or index within the system to facilitate back-end operations such as linking different tables within a database.

In the context of foundational systems, **ID numbers are considered to be “unique” when:**

1. the number-generating process ensures that no two people within the system share the same number; and
2. a deduplication process ensures that the same person does not have multiple identity records or numbers (i.e., that they are unique in the database).

In addition to their function as back-end identifiers, however, ID numbers have been used for authentication as a type of credential. In this role, they serve a similar function to that of a username: they are information that a person presents to a relying party—along with one or more authenticators such as biometrics, passwords, OTPs, PINs—to say “this is who I am.” The system then uses the ID number (or username) to look up the person’s record (or account) in a database and then verify the authenticators they have provided against that record. As discussed above in the case of **India**, using a unique ID number as an identifier during authentication could eliminate the need for physical credentials. However, there are certain limitations to this use including the need for connectivity and some people’s preferences for having physical credentials for in-person authentication.

Beyond usability, there are also important data protection concerns with using a “raw” (i.e., the root or original) ID numbers for authentication. Like user names, ID numbers can only be considered credentials in the weak sense, in that they are often widely known or easily discovered. The more these numbers are used across multiple systems, the higher the risks that they can be used to correlate information about a person. This risk is even higher when ID numbers are used as authenticators in addition to identifiers—i.e., when they are treated as a user name (identifier) in some systems, and a password (authenticator) in others. This has happened extensively in the **US** and **UK**, where—in the absence of national ID systems—social security numbers (SSNs) have become a *de facto* authenticator used to prove that a person is who they claim to be for services that lack a stronger authentication mechanism (e.g., asking people to provide the last four digits of their SSN when logging into online banking).

Alongside policy, regulatory, and legal controls that dictate the appropriate use of identifiers in order to avoid this type of function creep and its associated risks, technical measures should be adopted to obscure the ID number when it is used for authentication or other purposes. This may include, for example, using tokenized versions of the identity number—discussed below and in Box 21 on India’s virtual ID system—rather than the original ID number. In addition to evaluating the potential use of the ID number outside of record management, practitioners must also determine the structure of the number itself, which has implications for the system’s ability to protect privacy and personal data.

Number structure

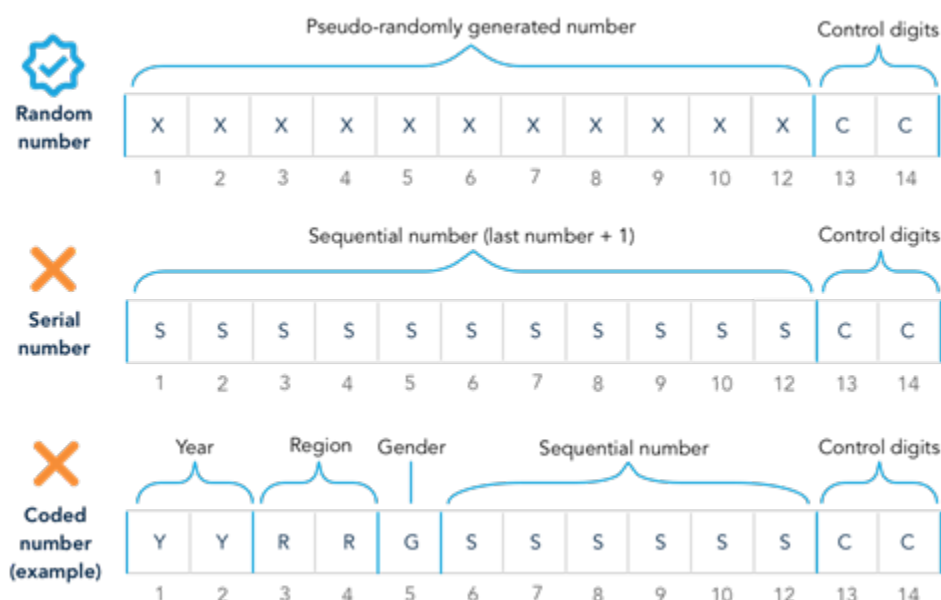
The structure of an ID number—including its format and length—require careful consideration of country context and privacy concerns. In any system, ID numbers can take one of three formats:

- **Random.** A random number (technically a “pseudo” random number) is generated using mathematical algorithms and contains no information about the person.
- **Serial.** A serial number is assigned based on the order of entry into the system, with the highest number assigned to the most recent enrollee.

- **Coded.** A number that contains information about the person, with certain digits coded based on attributes such as birth year, gender, nationality, and location of application.

Historically, many countries adopted coded numbers in their national ID and civil registration systems. In part, this was an innovation that helped standardize and pre-assign these numbers in the context of paper-based systems managed simultaneously by decentralized offices. In this context, coding numbers allowed for disconnected local offices to assign (relatively) unique numbers without knowing which numbers might already have been assigned by a neighboring office.

Figure 28. ID number structure



In the digital era, however, randomized numbers are the preferred choice for enhancing privacy and security. Connectivity between registration points, along with the centralized nature of deduplication and advanced computing power, mean that it is now possible to assign unique, random numbers to every person in the ID system. Random numbers offer three primary benefits over coded numbers:

- **They reveal no personal information.** By definition, coded numbers reveal information about a person. And while serial numbers reveal less information than coded numbers, they do—by virtue of being ordered—provide a relative indication of age. When accessed by administrators in a database or during authentication, the information these numbers provide could be used for profiling, discrimination, or social exclusion, even if it appears innocuous. For example, a number indicating the region where the individual was born could be used to infer ethnicity or religion if a particular group is predominant in that region. In contrast, random numbers reveal nothing about a person and therefore protect privacy by avoiding the data exposure. For this reason, random numbers are required under multiple frameworks, including **Europe's** eIDAS standards (see www.eid.as).
- **They are more secure.** Coded numbers make it easier for fraudsters to guess an ID number by narrowing down the possible combinations based on a few known facts about a person.

This is a particular concern in the age of social media, where basic information about a person (e.g., their age, name, gender, and location of birth) is relatively easy to determine. Because they contain no information about the person, random numbers (as well as sequential numbers) are not susceptible to this type of attack.

- **They are immutable.** In some cases, coded numbers contain information—such as nationality, place of residence, or gender—which may be subject to change over an individual's lifetime, requiring the numbers to be updated. In contrast, random and serial numbers can be constant from the point of entry (e.g., at birth) to retirement (e.g., after death) for each person in the system.

In addition to format, the length of an ID number has important implications for its utility. Key factors to consider in determining length include:

- **Population size and growth.** The number of digits selected should allow for more than enough numeric combinations to provide *new* (i.e., not recycled), unique numbers to all newborns and new arrivals expected in the foreseeable lifetime of the ID system. For example, an 8-digit number using numerals 0-9 would provide 100 million unique numbers, while 10 digits would provide 10 billion.
- **Use of control digits (or checksums).** Control digits are numbers computed from—and then added to—the randomly generated stem via a checksum or hashing function. They are used to check data entry errors (by a human) such as mistyped digits, transposition errors, etc. The more complex the hashing or checksum algorithm, the greater the ability to detect more types of errors (and the more control digits required).
- **Usability.** While longer numbers are needed to accommodate population growth (and control digits add to this length), excessively long numbers may compromise usability as a common identifier or authenticator—i.e., when people must remember the number, and/or when the number must be frequently entered by hand. This issue may particularly affect people with low levels of literacy.




Cards

Cards are perhaps the most common credential used for foundational—as well as functional—ID systems, including for national IDs, voter ID cards, social security cards, health insurance cards, and more. However, although ID cards are common and well-understood credentials, the process of choosing the type of ID card is far from straightforward, with myriad standards, features, and vendors offering different benefits and very different use cases. Not all cards are created equal, and the cost, security, durability, and utility varies dramatically from card to card, including—for example—whether the card has an integrated chip.

When designing a card, practitioners should consider the following, based on context-specific needs:

- Card materials and security features
- Machine-readability, including data storage and processing
- The visibility of data on the card

Table 32. Comparison of common card types

			
	Magstripe	2D Barcode (e.g., QR code)	Smartcard
Storage	Encodes up to 75 alphanumeric + 147 numeric characters	Encodes up to 500 bytes/inch ² , sufficient for fingerprint and cryptographic signatures	Depending on memory chip , can store 8kb-256kb
Internal computing	None	None	Microprocessor capable of cryptographic algorithms
Readability	Card reader	Camera (e.g., on a mobile phone)	<i>Contact:</i> card reader <i>Contactless:</i> RFID/NFC receiver
Digital authentication of user	Online against a server via internet or mobile services, offline against local system via app	Online against a server via internet or mobile services, offline against local system or barcode via app	Online against a server via internet or mobile services, offline against the chip (match on card)
Resilience to tampering	Low-medium based on material and physical security features	Low-medium based on material and physical security features; higher if barcode is digitally signed	High if built-in encryption and digital signature capabilities and certified (e.g. CC EAL) components are used
Cost per card	Low of ~US\$1.5/card , higher depending on material, security features	Low of ~US\$1/card , higher depending on material, security features	Typical range of ~US\$2-10/card (higher for contactless cards)

Source: ID4D *Technology Landscape*, *Digital ID Toolkit*, *Costing Model*, expert consultation

Materials and security features

Modern ID cards are usually made from synthetic materials, including **polyvinyl chloride** (PVC, common plastic cards), **composites** of PVC and **polyethylene terephthalate** (PET), **polycarbonate** (a thermoplastic material made up of layers of plastic), and **Teslin** (a synthetic, flexible paper substrate), all of which can be composited. Each of these materials has advantages and disadvantages. PVC, for example, is the cheapest material but also the least durable. Polycarbonate cards come at a higher price but can be more durable and more tamper-resistant than other materials. Meanwhile, certain types of PET are more durable to heat. Some security features can work better on certain types materials (e.g. laser engraving does not necessarily work as well on PVC as polycarbonate).

Cards made of any material can include **overt**, **covert**, and **forensic** security features (i.e., levels 1, 2, and 3) to make them more resistant to tampering or counterfeiting. Such features can add significant additional costs, and include, but are not limited to, hidden images or texts using ultraviolet or fluorescent printing; laser engraving (polycarbonate cards only; adding a semi-transparent copy of a photo or image (a “ghost image”); micro text printing; embossing; holograms, etc. Furthermore, some security features are proprietary to particular vendors, which could introduce some form of lock-in, and may not necessarily reduce risks of fraud. The choice of material and security features will be highly dependent on country context, including budget, concerns regarding fraud, and how long the cards will in circulation before renewal is required.



When determining the material and security features of a physical card (as well as whether a physical card is necessary), it is recommended that countries conduct a comprehensive cost-benefit analysis that take into account intended use cases and public consultation to understand the advantages and disadvantages of different approaches. See the costing model for a more in-depth description of the pros and cons of different card types and average prices based on material and security features.

Data storage/processing capacity

In addition to their material and security features, cards vary in terms of their technology for storing and/or processing machine-readable data—i.e., information that can be read by and interact with hardware and software. There are three main technologies that are used for machine-readability and data storage on ID cards, which can be used in isolation or combined on the same card:

- **Magnetic stripes (magstripes):** Historically used in for bank and credit cards, magstripe cards encode information in a magnetic stripe that can be read when it is swiped or inserted into a card reader. Although not as cheap as barcodes, magstripe cards are a simple alternative to more advanced smartcards, but they can only hold a very limited amount of data.
- **Barcodes:** One-dimensional (1D) or two-dimensional (2D) barcodes encode information that can be captured by a scanner or camera, respectively. While 1D barcodes (e.g. a barcode on the back of a product to be purchased in a store) are useful for storing short numbers (e.g., a 12-digit ID number), 2D barcodes—e.g., quick response or QR codes—have a higher data storage capacity. For example, they can store encrypted personal data, images, and a digital signature that vouches for the authenticity of the data. Some countries have attempted to encode a biometric template (e.g. fingerprint) into a 2D barcode to facilitate offline authentication, but this comes with significant privacy and data security risks—unless it is encrypted—because that data is easily readable. Barcodes are cheap to implement, as they are simply printed as part of the card personalization process. However, they are less secure than smartcards because they are externally visible and not dynamic.
- **Smartcards:** Cards with an embedded chip (i.e., “smartcards” or e-ID cards) offer the highest level of functionality, including the ability to store multiple applications and complete

cryptographic operations locally. As a result, data stored on a smartcard can be accessed offline for authentication, even where there is no internet connection or mobile network. “Contact” smartcards are read when inserted into a card reader, while (more expensive) “contactless” cards use radio frequency identification (RFID) or near field communication (NFC) to communicate with a receiver in close proximity. Access to the smartcard needs to be controlled for privacy reasons (and if fees are going to be charged for such access), which can be accomplished through software-based authorization or the integration of a Secure Access Module (SAM) chip loaded with relevant decryption keys into the smartcard readers.

Adopting one or more of these technologies is critical to using an ID card in a digital environment, including for:

- **Authentication of the person.** In addition to verifying the authenticity of the credential and its data, magstripes, barcodes, and/or chips can each facilitate automated authentication that binds the person to the credential, ensuring that they are its rightful owner. Of the above options, smartcards offer the most secure authentication capabilities, both online and offline. Magstripes and barcodes can effectively serve as an index that points to a person’s record in a database for online authentication. For example, people often swipe a magstripe card and enter their PIN at an ATM, and this information is then sent to the bank’s server to verify that the PIN associated with the card number (read from the stripe) matches the PIN the person has entered.
- **Verification of data and the card’s validity.** Machine-readable data stored in a magstripe, barcode, or chip can provide additional security against tampering and counterfeiting by attesting to the validity of the credential and its data. For example, the data stored in a magstripe, barcode, or chip can be checked against the information printed on the card or against a database (remote with an internet connection, or local without) to ensure that they match. Security is increased where this data is digitally signed by the issuing authority.
- **Storage of non-visible data and additional applications.** Smartcards and QR codes in particular have the capacity to store data that may not be visible on the card, such a unique ID number. Smartcards also have the capacity to store multiple applications, such as digital wallets that—combined with the chip’s microprocessor—can provide a variety of applications beyond identification and authentication. However, most countries that have attempted to introduce “multipurpose” smartcards—e.g., driving license and health information on the same card—have had limited success compared to promoting interoperability between information systems.

Visibility of attributes

In addition to the form and function of the ID card, practitioners must consider which data will be both (1) printed visibly on the card, and (2) accessible through a magstripe, barcode, or chip.

As with the collection of data, practitioners should seek to minimize the amount of personal information printed or stored on the card to that which is necessary for its intended use cases. Printed information is visible to anyone who has access to the card and therefore should therefore *not* include sensitive data or data that might increase the risks of discrimination, profiling and social exclusion (e.g., nationality, ethnicity, tribe, religion, gender, etc.). Countries should also consider not

printing “root” identifiers (e.g., a unique ID number in non-tokenized form) or information that could change often (e.g. address). Likewise, since the front of a card can often be photocopied or taken photos of, countries should consider separating information on the front and back faces. For countries where only a portion of transactions will involve digitally reading a card, some information (e.g., a photo, name, etc.) must be visible on the card. However, efforts should be made to minimize this information wherever possible.

In addition, practitioners can deploy technological solutions to limit who has access to which information stored digitally on the card. For most transactions, service providers only need access to a limited set of information. Restricting the visibility of unrequired attributes therefore limits the processing of personal data, increasing privacy and data protection. For example, an election official may need to verify a person’s name, age, and locality, but they may not need access to information such as the person’s full address, their fingerprint, or other information in the ID database or card. Smartcards in particular can allow for the selective disclosure of certain attributes, as card readers can be programmed to restrict access to specific categories of data—such as biometric data—to authorized users, or to the relevant attributes identified in a particular context. New solutions for different models of attribute-based credentials are continuing to develop and can provide additional options for the selective disclosure of only the attributes required for a transaction (see Box 35 for a current example from **Germany**).

Box 35. Selective attribute disclosure in the German eID system

The **German** eID system relies on **mutual authentication** of its eID card in order to protect privacy and ensure secure transactions. This means that both the card holder (e.g., a person attempting to prove who they are to a service provider) *and* the relying party or service provider authenticate themselves against the chip of the eID card.

The principle of mutual authentication allows both communication parties to: (1) have proof of the identity of the counterpart and (2) establish a trusted and secure end-to-end-protected channel between the relying party and the chip of the eID.

As part of the mutual authentication, the relying party has to **prove their authorization** to get access to the relevant data. Access to any data is only possible after successful authentication of the relying party and verification of the corresponding access rights. The authentication of the communication parties and the assignment of access rights are realized via dedicated public key infrastructures.

Because the personal data is securely stored on the eID card’s chip and transmitted via an authenticated channel, the authenticity and integrity of the data are ensured without the need to sign the data. This means that unlike signature-based eID schemes, the relying party receives no permanent proof of identity.

Source: https://www.bsi.bund.de/EN/Topics/ElectrIDDDocuments/German-eID/german-eID_node.html

Mobile ID

Mobile phones and other devices can also provide portable digital identity credentials capable of authenticating users for a variety of online and offline transactions. The prevalence of mobile phones and the relatively low cost of some mobile IDs compared to a card-based system can make this an attractive option. In many countries, however, it would be difficult to deploy a mobile ID solution as the *only* identity credential, given that not everyone has a phone and network coverage

may not be universal. Indeed, mobile-based systems are often deployed as optional or additional credentials to increase user convenience and choice.

Box 36. Moldova's Mobile eID

In 2011, the Government of **Moldova** embarked on a governance modernization program to transform delivery of public services using information and communications technologies (ICT). One core priority of this initiative was to offer e-service providers a simplified way to integrate strong authentication and signature functionality into their services. In order to accomplish this, the government adopted a **Mobile eID (MeID) solution along with a suite of shared platforms**, including MPass (for strong authentication and single sign-on functionality across government information systems and e-services) and MSign (used to electronically sign documents and records and validate electronic signatures).

MeID was launched in 2012 via a **PPP** that is described in Box 25. The MeID solution built on the existing PKI infrastructure and a strong foundational ID system, including the **State Register of Population (SRP)**, which covers virtually the entire population and assigns each citizen a 13-digit personal identification number at birth. The SRP is the core source for identification information and underpins numerous other registers and systems. In addition, the government issues physical ID cards (which as of 2014, includes the option of a smart “eID” card that also offers digital authentication and signature capability).

The MeID solution uses a **SIM-based or client-side model** to allow for mobile authentication and document signing. In order to enroll in this service, users first obtain a PKI-enabled SIM card through a mobile provider, who validates their identity against the SRP and generates a public and private key pair on the SIM. This SIM card then uses PKI encryption (i.e., digital signatures) to authenticate users via the MPass platform and secure e-signatures via the MSign platform. This solution provides a high level of assurance and legal force to electronic transactions, which can be used for a range of services including electronic tax filing, submitting electronic reports, and requesting e-services, etc.



Source: *Moldova Mobile ID Case Study*.

In general, there are five main options for implementing a mobile ID:

- **Smartphone apps.** Smartphone-based apps can hold a virtual version of existing identity credentials, allowing people to avoid carrying a separate ID card—e.g., similar to the “cards” a person adds to their Google or Apple Wallet. These credentials allow users to quickly access and share identity data, (e.g., via a QR code), and may also offer the ability to authenticate this identity via a PIN, OTP, or FIDO-certified authenticator. Both **India** and **Brazil** have recently deployed ID apps of this kind (see <https://aadhaarapi.com/maadhaar/> and <http://www.dni.gov.br/> for more information).
- **SIM-based PKI.** Similar to smartcards, this model uses a PKI-enabled SIM card that allows the owner to authenticate themselves *on* the mobile device by using (1) secure elements on a crypto-enabled SIM card to manage the private key, (2) the handset for the entry of an additional factor (e.g., a PIN) to authenticate the user, and (3) the mobile operator’s network to send the result to the relying party. This model is used in countries such as **Sweden**, **Finland**, **Estonia**, and **Moldova** (see Box 36). This method requires a PKI-enabled SIM card similar to the chips embedded in smartcards, but can work using any type of mobile phone, including feature phones and smartphones.
- **Server-side PKI.** In this model, authentication is done via a remote hardware security module (HSM) rather than on the mobile device itself, which means that a mobile phone with *any* SIM card can be used as long as it can send and receive SMS. When a user activates the service, a transaction authentication number (TAN) is generated remotely by the authentication authority and sent to the phone via SMS, along with a hash value of the authentication message. The user then compares the TAN and hash value, and—if they are the same—enters their PIN, and the server signs the message with the PIN and HSM. This is the model used in **Austria** (see Box 37).
- **FIDO-enabled devices.** In addition to running apps, FIDO-certified smart phones, laptops and tablets (which include all devices running Android 7 or higher and all Windows 10 devices) can provide secure multi-factor authentication (MFA) natively. FIDO MFA is enabled via a combination of an on-device biometric match or other “user gesture” such as a PIN to authenticate a person to their device, followed by a second factor—using public key encryption to authenticate against a server—that authenticates the device to the online service. This means that MFA can be delivered not only in a smartphone app, but also for transactions delivered via a browser; support for FIDO is embedded across all elements of the Android and Windows platforms. FIDO’s use of public key cryptography leverages a “lightweight” form of PKI.
- **Mobile network operator service.** A mobile network operator can provide an authentication service for its customers, based on their registered information and/or transactions. This could use a variety of different technologies and could or could not be linked with a country’s foundational ID system. For example, the GSMA—a global association of mobile network operators—have developed a Mobile Connect, which is a federated digital identity solution that uses APIs based on OpenID specifications to allow people to log in or authenticate themselves when accessing websites.

Box 37. The Austrian virtual Citizen Card

The **Central Register of Residents (CRR)** is a national information system that contains data about every resident of Austria (citizen and non-citizens). Austria mandates that all residents register their presence in the country, and the CRR contains the records of all these registrations. Each data record in the CRR has a 12-digit unique identifier, the resident's full name, sex, date of birth, citizenship, and full address. Records of foreigners also contain passport data.

While registration is mandatory, there is no equivalent requirement that every resident obtain a physical ID card. Instead, Austria has a **virtual Citizen Card (CC)** which can be installed on different devices, with smart cards and mobile phones being the two most prevalent interfaces used.

In order for a resident to use a smartcard-based CC, they need the activated CC, a card reader, a PC connected to the internet and special software (Citizen Card Environment- CCE) at the user end, and, a special software "MOA- ID" at the service provider end that helps with authentication.

Source: Slamanig, B. Z. 2013. On Privacy-Preserving Ways to Porting the. *FIP Advances in Information and Communication Technology*, (pp. pp 300-314), cited in *Privacy by Design: Current Practices in Estonia, India, and Austria*.

Credential Issuing

For people to use their credentials, they must first receive them. In some cases—such as user names, ID numbers, PKI-enabled SIM cards, and some non-smart cards—these could be issued instantly during registration and given to the user on the spot (or virtually via email) if identity proofing (including deduplication) can be carried out live. In other cases, credential issuing may take time or be done at a different location than registration, requiring a separate system of personalization, storage, and distribution. Depending on the method of issuance, a long lag between registration and credential issuance increases the chances that the person moves to another address and thus creates challenges to ensure that the right person receives the right credential.

The process for credential issuing is therefore important for the inclusivity and utility of the system, as well as its ability to guard against identity theft, fraud, and impersonation. Practitioners must decide how to personalize credentials—i.e., print, engrave, and/or encode them with information for each person—and distribute them in a way that is

- Cost effective and technically feasible for the ID provider
- Convenient for people
- Ensures that the true owners maintain total control over their own credentials

For physical credentials such as cards, there may be some instances when it is possible to issue these “on-the-spot” immediately after a successful registration, and before the person leaves the registration point. This is the most user-friendly scenario, as people will not need to wait for the credential or make subsequent trips to collect it. Furthermore, it reduces the risk of the person not receiving it by post or other means and can increase integrity by ensuring that the person who collects the card is the original applicant. At the same time, on-the-spot issuing requires the ability to complete all identity proofing and deduplication processes in real time, which necessitates connectivity, a robust core system, possibly live links to other systems, and sufficiently trained and skills frontline staff to manually adjudicate issues (e.g., matches detected during deduplication). It

also requires the equipment to personalize cards or other credentials. If a country is issuing smartcards, data can also be encoded locally (e.g., as in **Thailand**). However, on-the-spot issuance may be infeasible for certain card materials and security features that require larger or more specialized equipment. A significant risk with on-the-spot issuance is controlling the pre-personalized cards, the loss of which could create risks of forgery on legitimate cards.

Where the identity proofing process cannot be completed in real time, or where credentials cannot be personalized at the point of registration, there will need to be a distribution mechanism that allows people to securely collect their credentials at a later date. Delayed collection can be done through one or a combination of the following channels:

- **Pick-up points:** People may be required to return to a pickup point (e.g. where they registered or other locations) in order to collect their credentials at a later date, which could be predetermined (e.g. after 15 days) or notified when it is ready (e.g. by SMS or email) following identity proofing. There are two options for personalization: (1) credentials are personalized on-demand at the pickup point or (2) they are personalized centrally and distributed to pick-up points. For on-demand, the feasibility of this depends on the material and features of the credentials and the capabilities at pickup points (e.g. internet connectivity, electricity and space), and requires personalization machine and, for cards, pre-personalized cards available (and securely managed). Certain specialized cards may require larger and/or more expensive personalization machines (e.g., for laser engraving), which means that these need to be personalized centrally (or at several different locations in the country) and then distributed to pick-up points. It may also be preferable (e.g., to reduce security risks of the card distribution or during the very high demand in a short period that accompanies an initial mass registration) to do centralized personalization. However, in many countries, this has resulted in local offices with a backlog of cards that are never claimed. Therefore, if on-demand distribution can be implemented, this is often the best approach. For integrity reasons, card collection should require some method of authentication in order to bind the person to the credential.
- **Mail delivery:** Credentials can also be personalized centrally or at several decentralized locations (e.g. regions or provinces) and delivered to applicants by post (e.g., as done in **India**). This is typically a more user-friendly option than office visits, however it requires a context with a strong postal system and one where people have addresses (or local post offices know the population well enough to facilitate delivery). Countries considering this approach should consider how quickly they can complete the identity proofing process—and, if cards, also the personalization process—because the longer it takes for a credential to be distributed, the greater the risk that the applicant will have a new address. Mail delivery has the added benefit that, for systems where address will be a collected attribute, people are more likely to give correct addresses if these will be used to send them the card. However, this method of distribution is less secure, as mail can be tampered with and intercepted, and involves additional actors in what is already a complex process. Furthermore, it may require some form of remote (online) authentication to activate the identity and credential or for the holder to confirm receipt. During the initial mass registration, the scale of credentials to be distributed can potentially place a strain on the standard postal system, so countries should be prepared for backlogs or to augment the capacity of the postal system. As a public company and considering the economies of scale, postal services could potentially negotiate marginal prices for the distribution of credentials. An alternative

or complementary approach is to use the services of courier companies. Irrespective of the service provider or approach, ID agencies should ensure that relevant legal agreements are in place with performance standards, dispute resolution protocols, and clarity on respective roles and responsibilities.

- **Mobile units:** Certain countries (e.g., **Indonesia**, **Malaysia**, **Peru**, and **Thailand**) have mobile registration and/or credential distribution units (e.g. one-stop-shops) that periodically or on demand travel to remote communities and to the residences of elderly and people with disabilities who may face challenges accessing the two approaches above. Peru, for example, has boats to reach remote populations in the Amazon. Malaysia and Thailand bring card personalization equipment with them, so that the card can be personalized on-the-spot if the person has already been identity proofed or deduplicated and their identity can be authenticated. Mobile units can be used to supplement office visits or mail delivery to difficult-to-reach and vulnerable populations. As with office visits, this requires some method of authentication to ensure the identity of the person collecting the credential.

Importantly, delivery mechanisms should reduce barriers to collection as much as possible in order to facilitate inclusion. For example, by adopting multiple of the above approaches, countries can provide a choice to people when they register of how they want their credential delivered. Exclusion mitigation should also involve measures to reduce the indirect costs of collecting a credential, such as the ability to elect between multiple distribution channels, outreach to specific groups, and allowing people flexibility in where and when they are able to collect credentials. In addition, **first credentials should be free of charge**. Any delayed issuance process must also include notifications, procedures, systems, and grievance redress mechanisms to handle situations when a credential is lost at some point in the process.

Authentication mechanisms

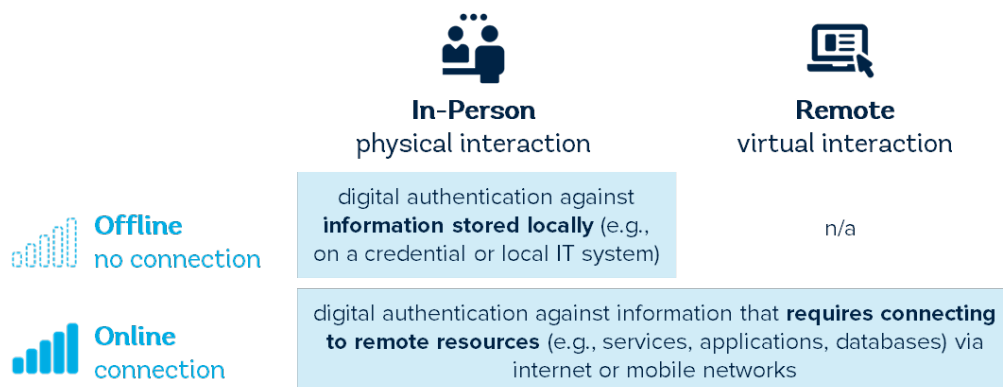
Authentication is the process of ensuring that an individual is the person that they claim to be. This involves matching a person's claimed identity—asserted through a credential (e.g., an ID card or unique ID number)—against one or more *authentication factors* that are bound to that credential. Potential authenticators include:

1. **Possession factors:** Something that a person demonstrates that they have, such as a physical or virtual card or certificate, or a hardware token.
2. **Knowledge factors:** Something that a person *already knows* (e.g., a challenge question or image) or *memorizes* (e.g., a password or PIN)
3. **Inherent factors:** Some physical attribute that a person can demonstrate that they have (e.g., a fingerprint or iris scan).

Secure authentication (i.e., for higher levels of assurance) requires a **multi-factor approach**. In general, the combination of authentication factors should include some or all of the three above categories. In addition, **sub-factors**—such as location (where are you?) and time (when are you trying to authenticate?)—can be used in combination with the other core factors to create further conditionality when authenticating.

Digital authentication—i.e., authentication that involves electronic credentials and processes—can be done **in-person** (e.g., at a physical bank branch or government office) or **remotely** (e.g., via a mobile or web service). While remote digital authentication is by definition “online” (i.e., it requires an internet connection), in-person transactions can be digitally authenticated using **online or offline** mechanisms (see Figure 29).

Figure 29. Digital authentication modes



Both online and offline authentication mechanisms have a common set of requirements in order to protect the person asserting their identity and to offer sufficient assurance to the identity consumer (a service, person, or relying party). In general, an authentication mechanism should:

- Respond only with a “yes” or “no” depending on the result of the authentication, rather than sharing and/or exposing PII, with the exception of special circumstances—such as complying with anti-money laundering (AML) regulations for customer due diligence (CDD)—subject to a person’s informed consent and comprehensive information security measures.
- Have known and easily accessible exception handling and grievance redress protocols in case the authentication mechanism fails (e.g., a false negative biometric result). A person should must never be denied a right, service, or entitlement (or their access made more difficult) as a result of a fault of the ID system.
- Facilitate the auditability of transactions, including tamper proof logs, certifying authentication devices, and identifying relying parties as well as potentially the individual operator within those organizations.
- Eliminate opportunities for the ID authority or other actors to use transaction metadata to track or profile the ID holder (e.g. through encryption, hashing, anonymization of data, decentralization of such data etc.).
- When identity data shared by the ID system and stored by the relying party as part of the authentication mechanism, ensure that information is secured in order to prevent loss or compromise.

- Implement security controls to reduce threats such as guessing, eavesdropping, replay or manipulation of communication by an attacker that could subvert the authentication mechanism.
- Be mandated by relevant laws and regulations, and the specific relationship between the ID system and the relying party be governed by a legal agreement (e.g., a memorandum of understanding) setting out respective responsibilities.

This section describes some offline and online authentication mechanisms that are commonly used in foundational ID systems. The choice of which mechanisms to adopt is closely tied to the types of credentials issued by the ID system and should be appropriate to the intended use cases for the system and country-specific constraints such as connectivity and digital literacy (see [Section II. Planning Roadmap](#)).

Offline authentication

Offline authentication—used for in-person transactions when connectivity is unavailable or unnecessary—must provide a means of verifying that the person asserting their identity is who they claim to be *without referring to other systems* (e.g. remote identity databases, online services, etc.) and, if possible, that the credentials they present are genuine. In general, there are three primary options for offline authentication (summarized in Table 33):

- **Manual (non-digital) comparison (i.e., taking an ID card at face value):** Traditionally, authentication processes have involved the manual inspection of credentials (commonly ID cards) to determine that they are genuine (e.g., via embedded security features) and assess whether the person or their physical signature resembles the photo or signature included on the credential. While this method is intuitive and requires less infrastructure (beyond providing the credentials themselves), it provides a lower level of assurance and more opportunities for corruption than digital authentication due to the potential for human error and/or discretion in applying the procedure. At the same time, this may be appropriate for certain low-risk transactions and/or the only viable solution in areas with no connectivity or electricity. If security features are to be a viable method of improving the reliability of authentication, relying parties need to be aware and appropriately equipped—e.g., in the case of level 2 (covert) security features, this might require a UV light.
- **Digital authentication against data stored on a smartcard:** Smartcards are capable authenticating a person offline with a higher level of assurance. In combination with card reader (or receiver, in the case of a contactless card) equipped with text input and/or a biometric scanner (e.g., fingerprint or iris), a comparison can be made between the presented authenticators (e.g., a PIN or fingerprint) and the data stored in the chip of the card. Matching can be done by the card's microprocessor itself or by the reader and associated software on the connected computer or device (e.g., a tablet or smartphone). Despite these benefits, however, smartcards can be expensive, and also require purchasing, distributing, and training operators on the use of card readers (e.g., POS devices). Some smartcards are being developed with their own embedded fingerprint scanner and power source, but these are very expensive. Smartcards used exclusively offline are also not necessarily much more secure than non-smartcard, as they could have been invalidated but continue functioning in isolation from the ID system. Furthermore, the security and integrity of data on a smartcard

cannot be guaranteed after they have been issued (e.g., in 2018 **Estonia** had to recall and reissue a significant proportion of smartcards in circulation because of a security flaw related to the private key stored on the chip). Indeed, many countries have issued smartcards without implementing this infrastructure, in which case they offer little benefit over “non-smart” cards.

- **Digital authentication via a 2D barcode:** Cards, certificates, or mobile apps with 2D barcodes (e.g., QR codes) also offer the possibility of digital, offline authentication when they are combined with readers and software that can match authenticators (e.g., PIN, fingerprint, photo) to those stored in the barcode itself or in a record in a local database that the QR code points to. In **India**, for example, the printed Aadhaar registration letters (“cards”) now include a secure barcode that contains biographic information and a low-resolution facial image of the Aadhaar holder in order to facilitate a manual comparison. Although QR-code documents may be cheaper than smartcards, they are less secure. For example, a photo can be taken of a QR code, which would compromise it. Likewise, they cannot store as much data and are limited to how much physical space they are allotted on the card. The higher density the barcode, the more likely that scratches or other damage will affect the ability of the data to be read without errors. Storing a fingerprint template on a QR code, for example, is likely to result in a very dense QR code and exposes the template to being replicated (e.g., printed on other cards). Another significant challenge with the use of barcodes for authentication factors in offline environments is the management of decryption keys: if a decryption key is widely available then an attacker can reverse engineer an applicable barcode to generate a fraudulent credential.

Table 33. Offline authentication mechanisms for in-person transactions

Type	Mechanism	Compatible Credentials	System Requirements
Manual	Visual comparison of a person to a physical credential	Any physical credential (e.g., a car or receipt) that has some information (e.g., a photo or signature) that can be compared to its bearer	Requires no equipment except the credential itself
	Comparison of authenticators to those stored on a 2D barcode	Physical or virtual cards (e.g., on a smartphone) or certificates with 2D barcodes + authenticators (e.g., PIN, biometric)	Input devices (i.e., card readers, text pads, fingerprint scanners, etc.) integrated in or connected to local device capable of matching the authenticators
Digital	Comparison of authenticators to those stored on a smartcard chip	Smartcard + authenticators (e.g., PIN, biometric)	Input devices (i.e., card readers with text pads and/or fingerprint scanners)

Online authentication

Where relying parties and users have access to internet and/or mobile network connections, online authentication can be used for both in-person and remote transactions. The ability to refer to other systems—such as remote servers, data stored in the cloud, web- and mobile-based applications, etc.—increases the variety of potential online authentication mechanisms, as shown in

Table 34, and the ability to check the validity of a credential. Ultimately, online authentication provides a higher level of assurance because it offers more potential authentication factors and a “live” source. At the same time, it may also bring greater data protection and cybersecurity risks.

The authentication level of assurance provided by online mechanisms varies according to the specific credentials, authenticators, and protocols used. In addition to choosing authentication methods with levels of assurance appropriate to the transaction, **practitioners must consider their accessibility and convenience**, particularly for vulnerable persons (e.g., low literacy, the elderly, and people with disabilities), and those with unreliable internet or mobile connections. For example, card-based authentication for remote transactions (e.g., e-services) would require the purchase and distribution of card and/or biometric readers to each person, which may be a barrier to adoption.

Table 34. Examples of online authentication mechanisms for in-person and/or remote transactions

Type	Mechanism	Compatible Credentials/Authenticators	System Requirements
Matching against a database (“ID on the cloud”)	Comparison of authentication factors to references stored in a central system	Numbers, user names, etc. + authenticators (e.g., PIN, biometric, password)	Input devices (i.e., keypad/board and/or biometric scanners) and secure network connection of relying party to central system
	Using public key encryption to authenticate against a server	Smartcard, card with 2D barcode, SIM card, or mobile device + authenticators (e.g., PIN, biometric)	Input devices (i.e., personal card reader/scanner, text pads and/or fingerprint scanners), PKI and secure network connection of relying party to central system
One-time passwords (OTP)	Password or PIN generated on demand for one-time use	Device that can receive the password (e.g., SMS on a mobile phone or smartphone/computer to receive an email or smartphone app that generates an OTP)	OTP infrastructure and secure network connection of relying party to central system
FIDO authentication	On-device match (fingerprint, iris, face, PIN) unlocks a private key used to authenticate against a server	FIDO-certified smartphone (e.g., Android, Windows) or external authenticator such as a FIDO Security Key + authenticators (biometrics or PIN)	FIDO-certified smartphone (e.g., Android, Windows) or external authenticator such as a FIDO Security Key, plus network connection between that device and the relying party’s systems

Federation

Federation is the ability of one organization to accept another organization’s identity credentials for authentication based on inter-organizational trust. The trusting organization must be comfortable that the other identity provider has acceptable policies, and that those policies are being

followed. Federation protocols and assurance and trust frameworks facilitate federation of digital identity between organizations. For federation to be effectively used globally, agreement and mapping with the ISO defined assurance framework and the adoption of standards are critical (Source: *Catalog of Technical Standards*).

Federation can occur at multiple levels:

- *A trusting organization can capture and send the credential to the issuing organization (i.e., an identity provider) for verification, to authenticate an identity.* After verification of the credential, the issuing organization sends a yes/no confirmation and may, when warranted and consented, send a set of claims giving information about the person, using federation protocols like SAML (security assertion mark-up language). For example, service providers in the UK can accept the credentials of multiple identity providers via the GOV.UK verify system (see Box 38).
- *A trusting organization can accept credentials issued by another organization, but still authenticate and authorize the individual locally.* For example, a passport issued one country is accepted as a valid credential by a receiving country (and could be validated, for example, through ICAO's global Public Key Directory or PKD), but the receiving country's immigration office still authenticates the holder and requires a visa to authorize travel.
- *A trusting organization can accept specific attributes describing an individual from another organization.* For example, a bank can request credit score from a credit bureau, rather than maintaining its own registry of credit information.
- *A trusting organization can accept an authorization decision from another organization (i.e., mutual recognition).* For example, a driver's license authorizing a person to drive in one location may be accepted by another location.

In order to establish a framework for federation, practitioners must:

- ☐ Establish a trust framework—i.e., a legally enforceable set of specifications, rules, and agreements that govern a multi-party system—that defines legal rules and operational rules (e.g., service-level agreements or SLAs)
- ☐ Determine federation protocols to be used (e.g., SAML or [Open ID Connect](#))
- ☐ Determine which attributes—if any—will be shared by the identity provider to the relying party/service provider upon successful authentication of the user. (For example, the combination of Open ID Connect and OAuth protocols allows for sharing different set of attributes, based on user consent.)
- ☐ Establish a secure communication channel between the relying party (service provider) and the identity provider to enable an authentication workflow between the service provider and identity provider application. This is typically done using digital certificates to secure communication and may also involve passwords (a shared secret) to authenticate the application.

- ❑ Manage the digital identities including expiration, revocation, and renewal

Box 38. GOV.UK Verify

Unlike many other countries, the UK has no single foundational ID system except for a civil registry. People hold a variety of credentials—such as driving licenses, passports, birth certificates, and more—and rely on some combinations of these to assert their identities for various purposes. In 2016, the UK government launched its GOV.UK Verify system to provide a digital identity layer that would allow UK citizens and residents to authenticate themselves online for a variety of public and private sector services.

Rather than relying on a single, centrally provided digital identity credential, the Government developed a federated system with multiple digital identity providers who are certified by the GOV.UK Verify platform to provide authentication services. GOV.UK Verify partnered with a number of private sector identity providers (e.g., banks) to issue digital identities with combinations of individual's various credentials and other “dynamic” proofs of identity as a foundation (e.g., micro-payments to a bank account controlled by the individual with a unique reference code, which requires the user to access their online banking system to retrieve the code and complete the proofing). The provider issues a digital identity along with varying credentials, including USB keys and mobile authenticators. People can then use this identity to authenticate themselves online for various services.

This system was designed with privacy in mind, as it allows people choice over their identity provider and prevents identity providers from knowing the precise service for which the authentication is being requested. In addition, it uses back-end tokenization at the point of transaction to avoid the correlation of Personal Identifiers (PIDs) across databases.

Source: Whitley (2018), ID4D Tokenization note (forthcoming).

Levels of assurance (LOAs)

A level of (identity) assurance is the certainty with which a claim to a particular identity during authentication can be trusted to actually be the claimant's “true” identity. Higher levels of assurance reduce the risk of a fraudulent identity and increase the security of transactions, but also can increase the cost and inconvenience to ID holders and relying parties, which could lead to exclusion. It is therefore imperative that practitioners consider the varying requirements of different use cases with respect to LOA. For example, biometric-based authentication is likely to be inappropriate for use across all use cases because some transactions (e.g., scheduling a medical appointment through a website) carry less risk.

Assurance levels depend on the strength of the Identity proofing process and the types of credentials and authentication mechanisms used during a transaction. For **identity proofing**, the level of assurance depends on the method of identification (e.g., in-person vs. remote), the attributes collected, and the degree of certainty with which those attributes are verified (e.g., through cross-checks and deduplication). For **authentication**, the level of assurance depends on the type of credential(s), the number of authentication factors used (i.e., one vs. multiple), and the cryptographic strength of the transaction.

Both eIDAS (*EU 2015*) and *ISO/IEC 29115* have developed standards to classify levels of assurance based on these processes and technologies.¹ In addition, recent guidelines from the U.S. National Institute of Standards and Technology (NIST) (*NIST 800-630-3*) have adapted this framework to separate out assurance levels for identity proofing (“identity assurance level,” or IAL) and for authentication (“authenticator assurance level,” or AAL), as shown in Box 39. In addition, the NIST framework distinguishes levels of assurance for the assertion of identity in a federated environment (“federated assurance level,” or FAL). While many systems will have the same level for each, practitioners can also select IAL, AAL, and FALs as distinct options, depending on the system requirements.

Box 39. NIST levels of assurance for digital ID

Identity proofing LOAs:

- IAL1: Attributes, if any, are self-asserted or should be treated as self-asserted; there is no proofing process.
- IAL2: Either remote or in-person identity proofing is required using, at a minimum, the procedures given in SP 800-63A.
- IAL3: In-person or supervised-remote identity proofing is required. Identifying attributes must be verified through examination of physical documentation as described in SP 800-63A.

Authentication LOAs:

- AAL1: Provides *some assurance* that the claimant controls an authenticator registered to the user. AAL1 requires single-factor authentication using a wide range of available authentication technologies. Successful authentication requires that the claimant prove possession and control of the authenticator through a secure authentication protocol.
- AAL2: Provides *high confidence* that the claimant controls authenticator(s) registered to the user. In order to authenticate at AAL2, claimants must prove possession and control of two distinct authentication factors through secure authentication protocol(s). Approved cryptographic techniques are required.
- AAL3: Provides *very high confidence* that the claimant controls authenticator(s) registered to the user. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 is like AAL2 but also requires a “hard” cryptographic authenticator that provides verifier impersonation resistance.

Federation LOAs:

- FAL1: Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography.
- FAL2: Adds the requirement that the assertion be encrypted using approved cryptography such that the relying party is the only party that can decrypt it.
- FAL3: Requires the user to present proof of possession of a cryptographic key reference to in the assertion and the assertion artifact itself. The assertion must be signed using approved cryptography and encrypted to the relying party using approved cryptography.

Source: *NIST SP 800-63-3*.

¹ The eIDAS framework is intended to be a reference for mapping EU ID systems for mutual recognition, rather than an implementation standard. Note also that ISO/IEC 29115 is in the process of being updated and the standards may shift.

The LOAs selected depend on the use case; some sectors and types of transactions will require higher levels of assurance than others. For example, changing an address may rely on a lower level of assurance than changing a password. Financial and health services often require a higher level of assurance than others due to the sensitivity of the data that is collected and maintained in those systems. **Ideally, the ID system's authentication architecture will be able to provide multiple levels of assurance appropriate to different use cases** (see Table 35 for examples).

Table 35. Example levels of assurance

	Low (level1)	Substantial (level2)	High (level3)
Identity assurance level (IAL)	Self-asserted identity (e.g., email account creation on web), no collection, validation or verification of evidence.	Remote or in-person identity proofing (e.g., provide credential document for physical or backend verification with authoritative source), address verification required, biometric collection optional	In-person (or supervised remote) identity proofing , collection of biometrics and address verification mandatory.
Authentication assurance level (AAL)	At least 1 authentication factor —something you have, know, or are (e.g., password or PIN)	At least 2 authentication factors (e.g., a token with a password or PIN)	At least two different categories of authentication factors and protection against duplication and tampering by attackers with high attack potential (e.g., embed cryptographic key material in tamper-resistant hardware token + PIN, biometrics with liveness detection + PIN/smart card)
Federation Assurance Level (FAL)	Permits the relying party to receive a bearer assertion from an identity provider. The identity provider must sign the assertion using approved cryptography	FAL1 + encryption of assertion using approved cryptography	FAL2 + user to present proof of possession of a cryptographic key reference in the assertion
Level of risk taken by relying party	mitigated	low	minimal

The selection of LOAs—and the identity proofing processes, types of credentials, and authentication mechanisms that enable them—should be based on a number of factors, including:

- The **likelihood** of a failure, breach, or unauthorized release of sensitive information
- The **risk** to individuals, institutions, programs, public interest if a failure or breach occurs—i.e., based on the level of sensitivity of the service/information and the expected level of harm
- The **convenience** and **inclusivity** of the identity proofing and authentication processes, as higher LOAs could increase the likelihood of exclusion errors.

LOAs are particularly important for federation and mutual recognition across borders, where an ID system must meet a particular level of assurance in order to qualify for recognition for a given purpose.

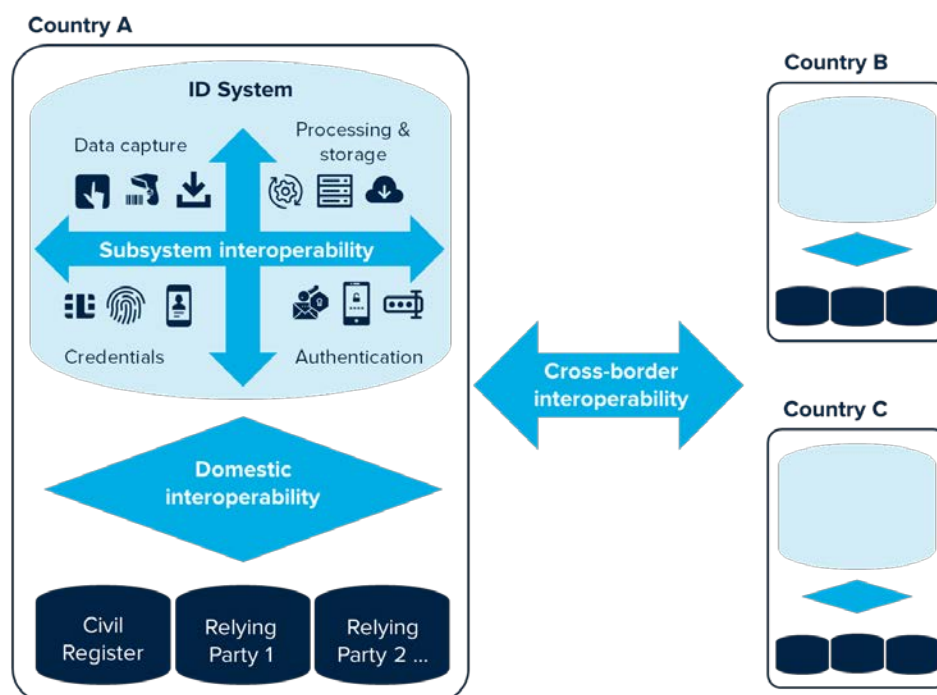
INTEROPERABILITY

Interoperability is crucial for developing efficient, sustainable, and useful identity ecosystems. Specifically, interoperability is the ability of different functional units—e.g., systems, databases, devices, or applications—to communicate, execute programs, or transfer data in a manner than requires the user to have little or no knowledge of those functional units (*ISO/IEC 2382*).

For ID systems, this occurs at three levels (see Figure 30):

1. **Between ID subsystems (components/devices).** Within the ID system itself, standards-based technical interoperability allows different components and devices to communicate with each other and work together. This includes, for example, interoperability between fingerprints captured with a scanner device and the deduplication engine, interoperability between smartcards and readers, interoperability of biometric formats captured during registration with those captured during authentication, interoperability between images captured by devices from different vendors, etc. (For more, see the Catalog on Technical Standards, or [Section III. Standards](#)).
2. **With other domestic systems.** ID systems must be interoperable with other systems—such as the civil registry and service providers that are relying parties of the system—in order to exchange data or facilitate queries. Communication with other systems may be provided through various interoperability layers, web services and APIs, or direct connections. (For example, see Box 40 below on the **Estonian** X-road model).
3. **With ID systems in other jurisdictions.** Cross-border frameworks for interoperability and mutual recognition allow credentials from one country to be accepted in other countries. This includes, for example, the acceptance of standards-compliant passports across the globe (covered by the *ICAO DOC 9303* standard), as well as regional frameworks for the mutual recognition of ID credentials—e.g., the **European Union's** electronic identification and trust services for electronic transactions in the internal market (eIDAS) regulations.



Figure 30. Types of interoperability in an ID system

Interoperability of these three types provides multiple benefits:

- **Promoting technology and vendor neutrality:** Using common standards for subsystem interoperability allows for a modular architecture and interoperability between devices, hardware, and software from different vendors. The ability to “plug-and-play” different components reduces the risk of vendor lock in and helps increase data portability across systems.
- **Improving the integrity of identity data:** Interoperability with the civil register is crucial for keeping identity data up-to-date with new births and/or deaths and reducing the need for costly re-enrollment or updating exercises.
- **Creating administrative efficiencies:** The ability to exchange data and make queries via domestic interoperability frameworks allows organizations to avoid duplicate data collection—e.g., to implement a “once only principle”—and inefficient, paper-based identity verification procedures. Domestic and cross-border interoperability allows applications to accept the ID provider’s credentials under a framework of mutual trust—within country or across borders—creating efficiencies in management of credentials and personal data.
- **Reducing fraud and improving targeting:** For e-government, social protection, taxation, healthcare, other services, data exchange and queries facilitated by a domestic interoperability framework can help verify and rationalize beneficiary information, prevent duplicate registration, and identify previously excluded individuals.
- **Improving end-user experience:** Where domestic and cross-border interoperability streamline data collection and administrative processes, it can also improve service delivery

and convenience for end-users. For example, people may no longer need to repeatedly give the same information to multiple organizations or—in the case of mutual recognition—apply for multitudes of different credentials.

- **Enabling innovation and new use cases:** When systems are interoperable—both in terms of subsystems and the interoperability of the ID system with other domestic or cross-border systems—this opens up the possibility of new applications and services that can be easily built on top of existing ones, which is less possible with a closed system.

Despite these benefits, the data exchange and links between systems that interoperability facilitates can create risks to privacy and data security. To mitigate these risks, some systems limit data sharing to the absolute minimum necessary or prohibit the propagation of a common unique identifier in order to reduce the ability to link information across databases. At a minimum, strong legal, regulatory, and governance structures—along with data subject consent and security and access controls to prevent data theft and regulate authorized use—must be in place to ensure that data transfers or other interoperability measures do not infringe on individual rights with regard to privacy and do not unduly put personal data at risk of theft or misuse.

The remainder of this section focuses on key issues with regard to the interoperability of the ID system with other domestic and cross-border systems, including:

- The requirements for setting up an interoperability framework
- Linking ID and civil registration
- Mutual recognition of IDs across borders
- APIs and data exchange layers (coming soon!)

For more information on subsystem interoperability, see [Section III > Standards](#).

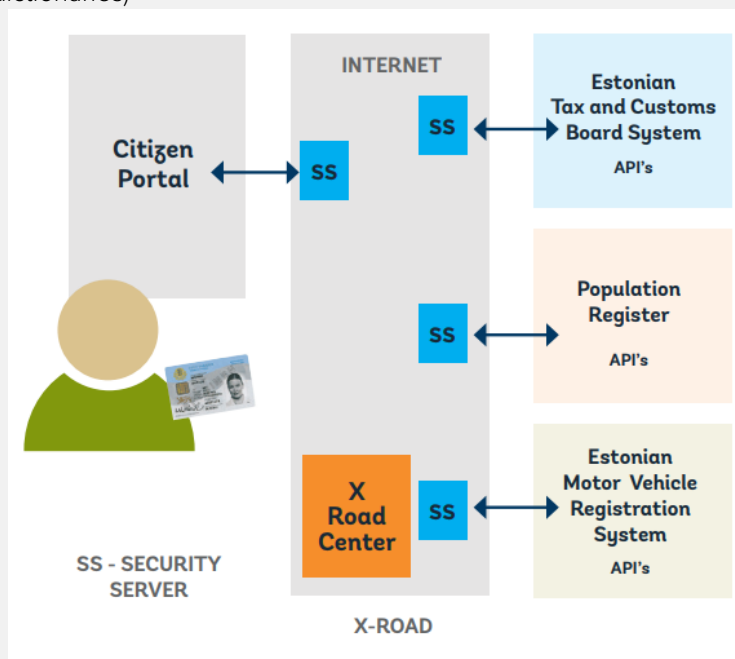
Box 40. Estonian X-Road Model

One pioneering example of domestic and international interoperability is **Estonia's X-Road system**, which is a centrally managed, distributed data exchange layer that enables information systems to securely exchange information over the public internet. X-Road is an open-source solution that has been adopted by a number of countries and is publicly available on GitHub (<https://github.com/nordic-institute/X-Road>). In Estonia, the ability to exchange data over X-Road has allowed the government to adhere to the “only once” principle of e-government service delivery and data collection, which dictates that public sector providers should not collect data that is already available from an X-Road ecosystem member, increasing administrative efficiency and user-friendliness, and limiting the processing of personal information. Backed by a strong regulatory framework, administrative system and the technological architecture, X-Road enables secure exchange of data between systems in alignment with the privacy and data protection principles.

At the core of the X-Road architecture is the RIHA (Administration system for State Information System) information system, which serves as a catalogue for the government's information system and provides the following:

- The information systems and databases that make up the public X-Road ecosystem
- Data collected and processed by these information systems
- Services, including X-Road services, provided by these information systems and the list of users of these services

- Responsible and authorized processors of the information systems and databases, and the contact details of people
- Legal basis for the database operations and processing
- The reusable components that ensure the interoperability of information systems (XML assets, classifications, dictionaries)



How X-Road Data Exchange works:

1. A user wanting to use an online service authenticates their identity via the citizen portal using their digital ID (smart card or mobile ID). A single sign on solution enables the user to request service from any department seamlessly.
2. Using X-Road, the service obtains the data needed to process the service request from other databases.
3. The Security Server component of the requesting system encrypts the data and sends it to the system (database) from which data are desired over internet.
4. The Security Server at the data provider system end authenticates the requesting system and if the authorization check succeeds forwards the request to the system.
5. The Security Server of the data provider system timestamps, digitally signs and logs the transaction and sends encrypted response, provided by the data provider system, to the security server of the requestor system.
6. The Security Server decrypts the response and then the service processes the request based on data fetched in real time and returns the response to the user.

Source: *Privacy by Design: Current Practices in Estonia, India, and Austria.*

Interoperability frameworks

Developing an interoperability framework requires a multi-stakeholder process and a long-term vision for the ID system. As per [the European Interoperability Framework](#), there are four interoperability layers that need to be defined:

- **Legal interoperability**—Legal, policy, and regulatory frameworks define the scope of interoperability, particularly with regard to data exchange and requirements for privacy and data protection.
- **Organizational interoperability**—For interorganizational-interoperability, federation, or mutual recognition of ID systems, organizations must define trust frameworks and process standards around the identity lifecycle (e.g., the eIDAS standards).
- **Semantic interoperability**—To ensure that the meaning of exchanged data and information is consistent, systems must adopt the same data standards or construct data dictionaries.
- **Technical interoperability**—To enable machine-to-machine communication, systems must adopt the same technology standards for software, physical hardware components, and systems and platforms.

Throughout these four layers, interoperability frameworks also rely on crosscutting **integrated public service governance** to ensure usability, security, privacy, and performance. Table 36 provides an overview of key requirements for defining each layer of the interoperability framework.

Table 36. Requirements for building interoperability frameworks

Layer	Requirements
Legal	<p>Perform “interoperability checks” by screening existing legislation to identify:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Interoperability barriers: Sectoral or geographical restrictions in the use and storage of data, different and vague data license models, over-restrictive obligations to use specific digital technologies or delivery modes to provide public services, contradictory requirements for the same or similar business processes, outdated security and data protection needs, etc. <input type="checkbox"/> Coherence: Evaluate compatibility between the enabling legislation of different organizations in order to ensure interoperability <input type="checkbox"/> Digital applicability: Ensure that legislation suits digital (as well as physical) identity data processing
Organizational	<p>Define inter-organizational relationships and processes:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Organizations must align their business processes, responsibilities and expectations to achieve commonly agreed and mutually beneficial goals and document them. <input type="checkbox"/> Clearly define relationship between service providers and service consumers e.g. MoU’s, Service Level Agreements (SLAs), API specifications, etc.

Semantic	<p>Adopt data standards to be used by organizations in the interoperability framework:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Develop semantic vocabularies and schemata to describe data exchanges, and ensure that data elements are understood in the same way by all communicating parties (e.g., via XML and JSON languages, and the use of metadata) <input type="checkbox"/> Define syntactic format of the information to be exchanged in terms of grammar and format.
Technical	<p>Adopt technical standards to be used for system components and devices:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Use open specifications, where available, to ensure technical interoperability <input type="checkbox"/> Put in place processes to select relevant standards and specifications, evaluate them, monitor their implementation, check compliance and test their interoperability. <input type="checkbox"/> Use a structured, transparent, objective and common approach to assessing and selecting standards and specifications, considering the requirement to make them consistent across borders <input type="checkbox"/> Consult relevant catalogues of standards, specifications and guidelines at national and regional level, when procuring and developing ICT solutions
Integrated public service governance	<p>Throughout the above layers, ensure coordination and documentation of:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The definition of organizational structures, roles and responsibilities and the decision-making process for the stakeholders involved <input type="checkbox"/> The imposition of requirements for aspects of interoperability including quality, scalability, availability, service level agreements, security and privacy controls <input type="checkbox"/> Change management plans that define the procedures and processes needed to deal with and control changes <input type="checkbox"/> Business continuity/disaster recovery plans to ensure that digital public services and their building blocks continue to work in a range of situations (e.g. cyberattacks or systems failures)

Linking ID and civil registration

One of the primary systems with which ID systems should interoperate is CR. Although CR and ID systems have a different focus (see Box 41), they are mutually reinforcing, and the accuracy and sustainability of an ID system is significantly enhanced by being interoperable with a CR system that is universal, timely and accurate. For example, a newborn should have a legal identity from birth, and an ID system should know when someone has died so their identity cannot be fraudulently assumed. At a minimum, interoperability and broader coordination with the CR is needed to ensure the accuracy of identity data over time. Furthermore, interoperability may be one of multiple linkages between ID and CR systems that help to provide access to proof of legal identity to everyone within a jurisdiction throughout their lifetimes.

Box 4.1. Understanding CR and ID

As defined by the United Nations, **civil registration** is the ... continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements of each country (UNDESA 2014, p. 65).

In practice, this means that the scope of civil registration is **vital events that take place within the territory or jurisdiction** (and potentially also for citizens abroad). As a result, they do not cover people for whom vital events—e.g., birth, death, marriage—did not take place within the country, such as migrants and refugees.

In contrast, digital ID systems and the population registers or databases on which they are based are designed to **cover people residing in the territory or jurisdiction regardless of where they were born** (or sometimes a subset of this population, such as adult citizens). They are therefore inherently dynamic. While the unit of importance in a CR system is the *event*, the unit of importance in an ID system is the *person*.

Furthermore, because the primary goal of ID systems is to identify people, they involve additional processes, such as the **capture of certain data** (e.g., biometrics) and **identity proofing**, as well as the **issuance of credentials** that are designed to be used for **authentication during transactions**.

Technical interoperability and broader coordination between ID and CR can take multiple forms, including:

1. Creating an identity record in an ID system through birth registration
2. Notifying an ID system of the legally-recognized death of an individual through death registration
3. Updating biographic attributes in an ID system based on vital events (e.g., marriage registration).

Furthermore, cooperation between ID and CR can also extend to joint administration which is discussed further under [Section III. Administration](#).

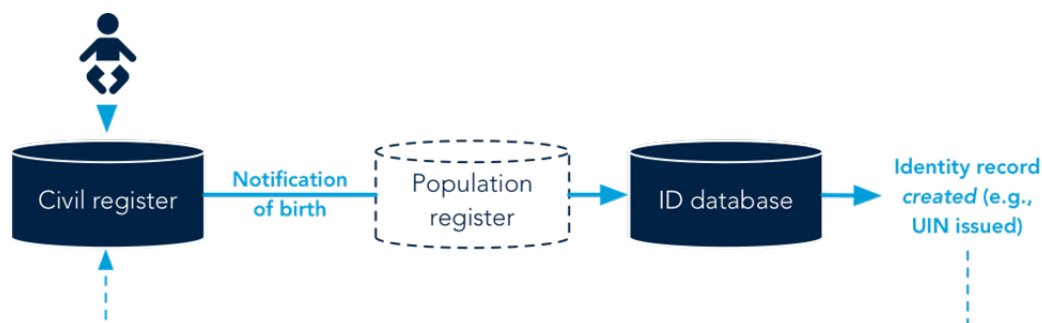
Data exchange or notifications from CR to update identities

Timely updating of existing ID records based on the CR is critical for ensuring the integrity of data over time and avoid costly re-registration and updating campaigns. Notifications regarding the death of a person following death registration are particularly important, as this allows the ID system to retire these identities and reduce instances of fraud. Updates could also include notifications of new births (where birth registration is linked to the creation of an identity), and other error corrections. Importantly, legal and technical controls for data protection and privacy need to be in place for any data-exchange between CR and ID, particularly because most civil registers collect more (and more sensitive) data than ID systems for statistical purposes (e.g., information of relative, birth weight, cause of death, etc.).

Figure 31. Interoperability between CR and ID for death notifications

Linking ID creation to birth registration

In some cases, countries have opted to issue identities from birth as part of or triggered by the birth registration process. This could include, for example, the generation of a UIN for a newborn by the ID system, following a notification—again, through a direct connection or open APIs—of a child’s birth. In some cases, this UIN could then be communicated back to the civil register. By seamlessly creating a digital ID from birth during the birth registration, this process can help ensure the inclusion of people of all ages in the ID system, increase the consistency of identities over time, and help incentivize birth registration.

Figure 32. Linking ID creation to birth registration

A “stock and flow” approach to simultaneously strengthen ID and CR systems

When introducing a foundational ID system, countries should assess the readiness of the CR system to support such an effort. For example, the CR system should be sustainable, sufficiently digitalized and the data it holds should be reliable enough to play a role in the Identity proofing process. However, CR systems in many countries—particularly low- and middle-income economies—have historically been of poor quality and low coverage because of, for example, underinvestment, legacy legal frameworks and processes, and limited incentives for people to register their vital events and for governments to strengthen CR systems. As a result, many people alive today were not registered at birth or their birth registration records have been lost or destroyed. Many people only register a birth when they have to (e.g., to apply for their first passport, which requires someone to prove where they were born). Likewise, a country’s CR system only covers births and other vital events that have occurred in that country’s territory and jurisdiction (that may also include vital events of nationals residing overseas), which means that migrants and refugees who were born overseas are most likely to be excluded.

Countries have therefore implemented practical alternatives to provide establish legal identity of their existing population (i.e., the “stock”) and new arrivals from outside the territory through implementing foundational ID systems or legally recognizing functional IDs issued by the private sector or international organizations with relevant mandates (e.g., refugees registered by UNHCR). **In the long-term, countries must improve CR systems to ensure the universal and timely registration of births of young children and future newborns, and of deaths (i.e., the “flow”).**

As discussed in *Section III. Registration & Coverage*, a country with an underperforming CR system and non-universal coverage should *not* necessarily require the applicant to have been registered at birth or to have a birth certificate before they can access a foundational ID system. Such requirements create barriers and unnecessary costs to accessing the foundational ID system and will lead to exclusion. When the foundational ID system reaches a steady state, however, it can be linked with the CR system to ensure timeline updates based on deaths and other vital events and—if desired—the creation of unique identities linked to birth registration. The “stock and flow” approach of simultaneously building a foundational ID system and strengthening CR systems is a practical one. Furthermore, it creates an opportunity to make a strong business case for investments in a CR system because a well-functioning CR system underpins the accuracy, sustainability and efficiency of a foundational ID system.

Mutual recognition of IDs across borders

When IDs issued by one country are recognized by other countries—whether for face-to-face or online transactions—they become a powerful driver of economic and regional integration, including to promote safe and orderly migration. Importantly, ID systems can be mutually-recognized without the need for harmonization into a common system through the use of minimum standards to facilitate interoperability and legal and trust frameworks (e.g., for levels of assurance) to set rules and build confidence in respective systems.

A key use case is migration, through which a physical or digital identity credential can be recognized as a travel document in lieu of a traditional passport. In Latin America, for example, **MERCOSUR** member States recognize each other’s ID cards (which meet *ICAO Doc 9303* standards as machine-readable travel documents) at borders in lieu of a passport, and a similar arrangement exists between **Kenya, Rwanda** and **Uganda** in East Africa. The benefit of recognizing cards from foundational ID systems as a travel document—particularly within regional blocs—is that they are more accessible and practical than a passport because people should have one by default, rather than a passport that requires a fee and often can only be applied for in major urban centers.

Another important use case is cross-border electronic transactions as part of the digital economy, which can be facilitated when a digital identity issued by one country is recognized for transactions online in another country. With an increasing number of transactions moving from face-to-face to online, and with the digital economy emerging as a key driver of economic growth, mutual recognition of digital identities between countries can accelerate trade in digital services and products and expand markets. For example, someone could open a bank account, register a business, and electronically sign contracts to trade in another country without ever needing to set foot in that country. The most notable example of this is the **EU’s** electronic Identification, Authentication and trust Services (eIDAS) regulation, which came into force in 2016 (see Box 42).

Box 42. The European Union electronic Identification, Authentication and trust Services (eIDAS) regulation

eIDAS provides a predictable regulatory environment, standards, and governance mechanisms to enable secure and seamless electronic interactions between businesses, citizens and public authorities in the **European Union**. It ensures that people and businesses can use their national electronic identification schemes (eIDs) to access public services in other EU countries where eIDs are available. eIDAS also creates a European internal market for electronic Trust Services (eTS) by ensuring that they will work across borders and have the same legal status as traditional paper based processes. eID and eTS are key enablers for secure cross-border electronic transactions and central building blocks of the European

The eIDAS Network consists of a number of interconnected eIDAS-Nodes, one per participating country, which can either request or provide cross-border authentication. Service Providers (public administrations and private sector organizations) may then connect their services to this network by connecting to the eIDAS node, making these services accessible across borders and allowing them to enjoy the legal recognition brought by eIDAS.

It is the responsibility of each country to:

- a) Implement their eIDAS-Node.
- b) Support the connection of national Identity Providers and Attribute Providers to the eIDAS-Node, thus making their national eID schemes accessible to cross-border online services.
- c) Notify the European Commission of their eID scheme (which could be a national ID or any other functional ID like a driving license), including its assurance level, to show that it complies with the eIDAS regulations for cross border services.
- d) Peer review the eID scheme notified by other member countries

In practice, eIDAS means that people with a digital identity from a system notified by a member State to the European Commission can use that digital identity to access any service available online from any location. For example, a German can register a business or land in Malta or an Austrian can open a bank account in the France, using the IDs issued by their home country.

Source: *EU (2015)*. See <https://www.eid.as/home/> for detailed information on eIDAS regulation and implementation.

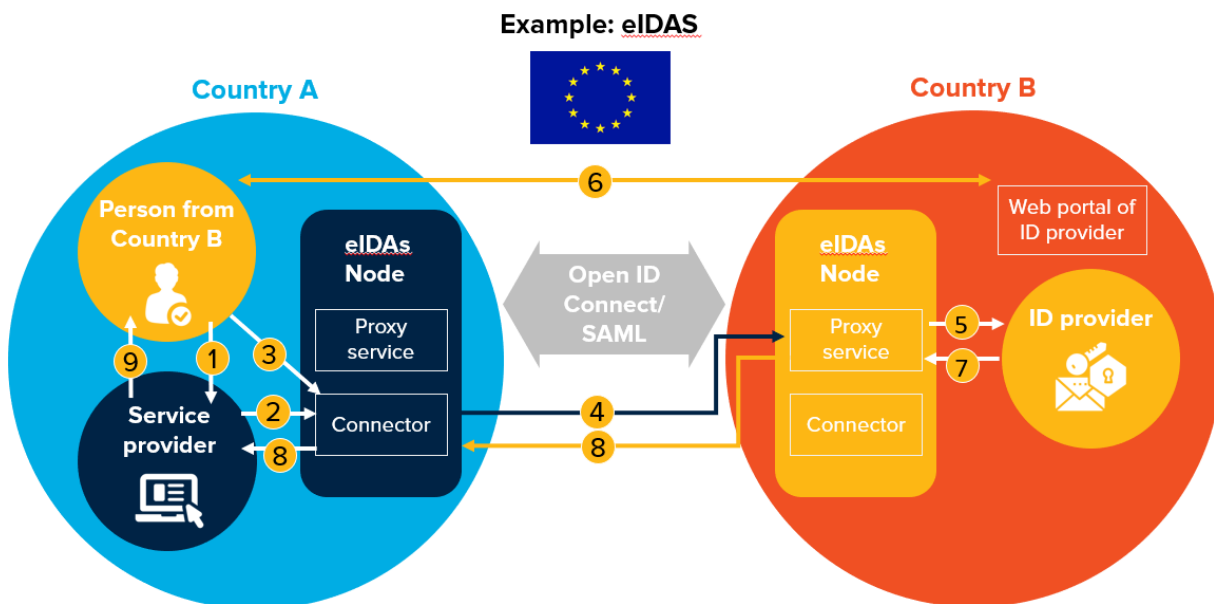
Several other regional blocs—notably the **African Union (AU)**, the **Economic Community of West African States (ECOWAS)**, the **East African Community (EAC)** (see Box 43), and **Association of Southeast Asian Nations (ASEAN)**—are now looking at options for mutual recognition of ID credentials across borders. Based on World Bank research, there are three broad potential architectures to facilitate mutual recognition while maintaining national sovereignty and without the need for harmonization:

1. **Web-based.** Online web-based authentication using federation protocol (SAML or Open ID connect); similar architecture used under eIDAS.
2. **API-based.** Online authentication using an API approach; similar architecture used among some Latin American countries.

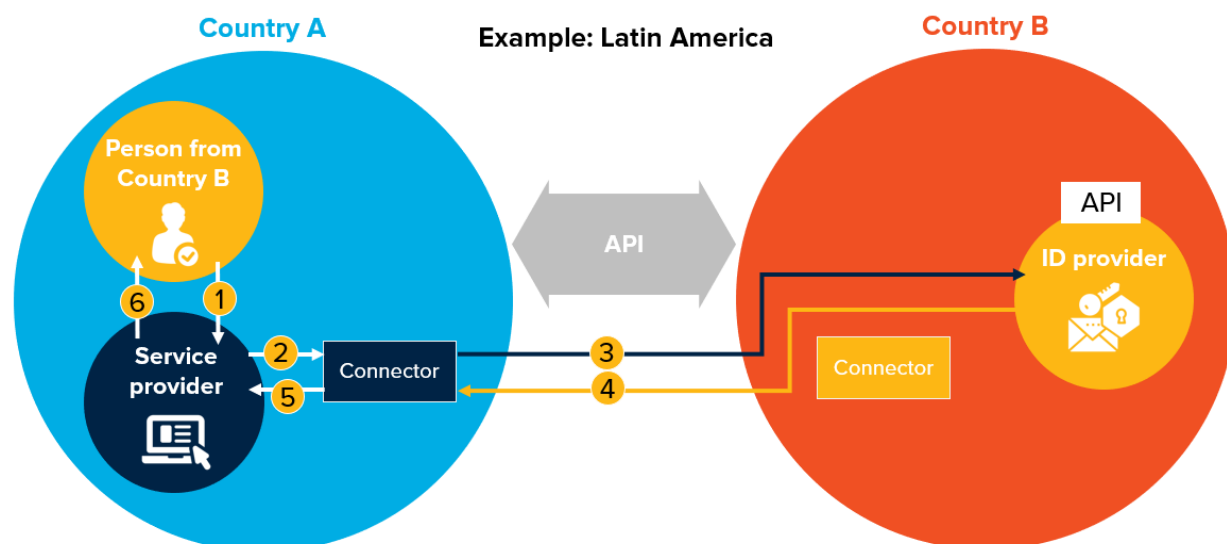
3. **Public-Private Key-based.** Offline and online authentication verifying the private key on a credential against a public key directory; similar architecture used for the ICAO Public Key Directory of electronic passports.

The architecture and workflows of these three options are illustrated below in Figure 33, Figure 34, and Figure 35.

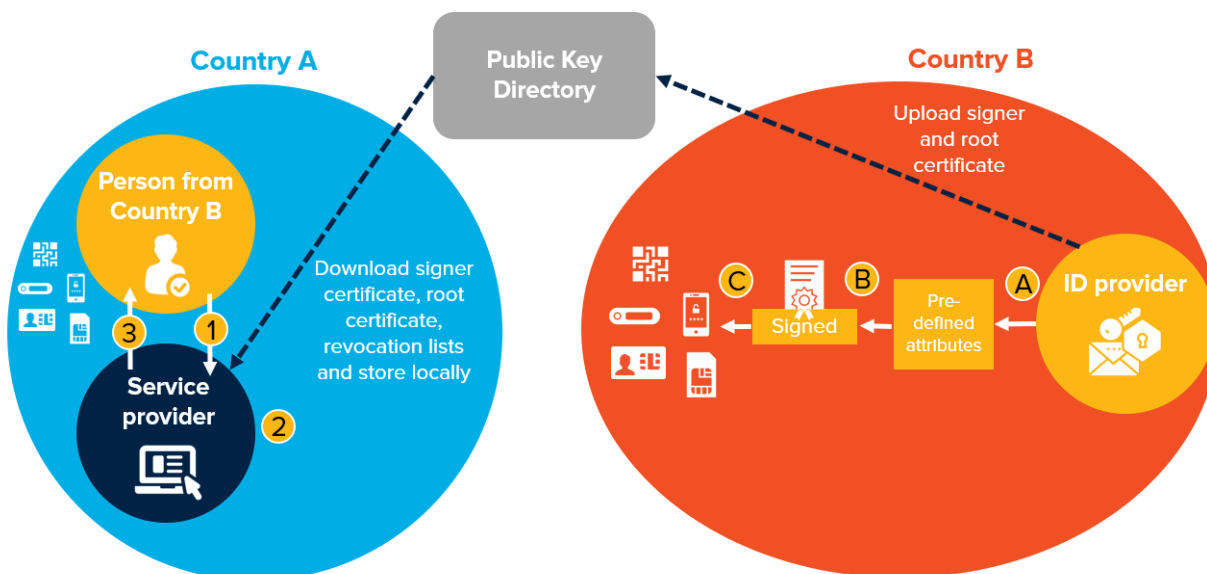
Figure 33. Web-based mutual recognition—example architecture and workflows



Web-Based Mutual Recognition – Authentication Flow	Prerequisites
<ol style="list-style-type: none"> 1. Person from Country B requests access to a service on a browser through the service provider's website in Country A (any location, any device). 2. Service provider's website sends the request to its own Connector (A). 3. Connector A asks the person for their country of origin, if not already provided. 4. Request is forwarded to the Proxy Service of Country B. 5. Proxy Service B sends the request to Identity Provider B for authentication (the person's browser is redirected to the identity provider's login page). 6. The person logs in. 7. Once authenticated, a response is returned to Proxy Service B 8. Proxy Service B sends a SAML Assertion to the requesting Connector A, which forwards this response to the Service Provider (the person's browser is redirected to the Service Provider's website). 9. The Service Provider grants access to the person. 	<ul style="list-style-type: none"> ▪ Internet connectivity ▪ Federation protocol implementation—SAML or Open ID Connect Server (eIDAS-node) ▪ Web portal for user authentication to be provided by identity provider ▪ Digital literacy of people to authenticate using password/OTP/PIN/FIDO authenticator of website

Figure 34. API-based mutual recognition—example architecture and workflows

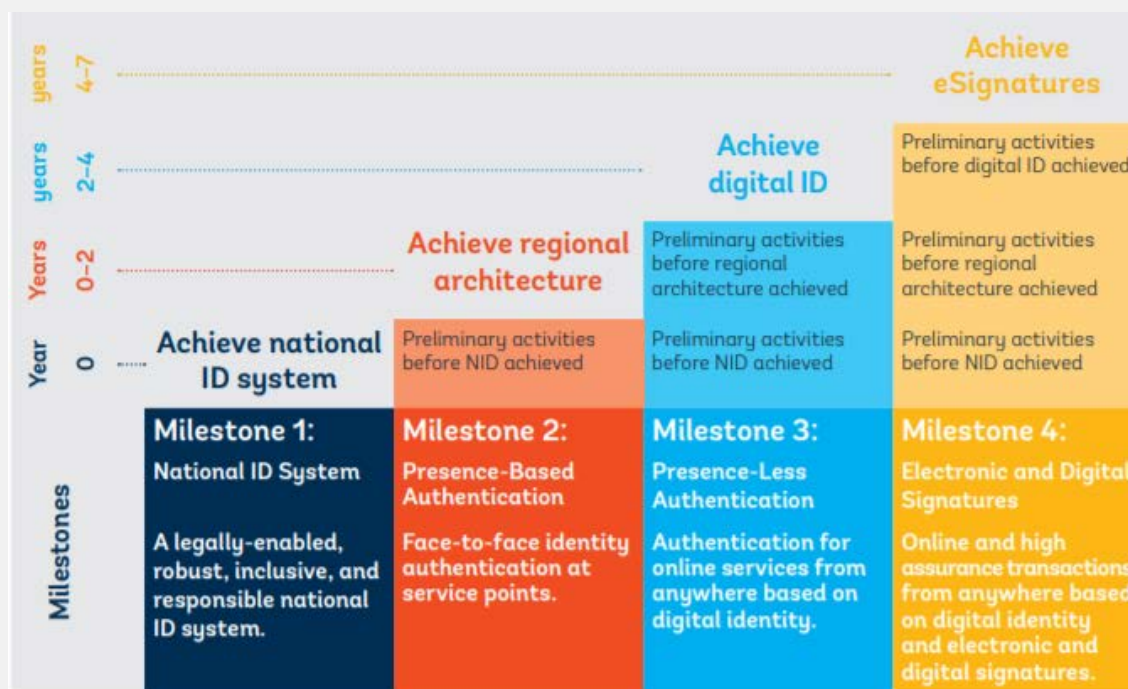
API-Based Mutual Recognition – Authentication Flow	Prerequisites
<ol style="list-style-type: none"> 1. Person from Country B provides country name, identification number, credential (e.g., fingerprint or OTP) to the Service Provider in Country A. 2. Service Provider sends the request to their Connector A. 3. Connector A sends the request to the Identity Provider of Country B. 4. Identity Provider authenticates the person and sends response to Connector A. 5. Connector A forwards the response to the Service Provider. 6. The Service Provider grants access to the person. 	<ul style="list-style-type: none"> ▪ Internet connectivity ▪ Authentication API to be provided by Identity Provider ▪ A connector component to route requests to the Identity Provider of the respective country ▪ In-person authentication (e.g., biometrics, OTP, PIN)

Figure 35. Offline mutual recognition—example architecture and workflows

Offline Mutual Recognition – Authentication Flow	Prerequisites
<p>Credential Issuance:</p> <p>A. The attribute/claims which will be used in a credential to establish identity are predefined by ID agency in coordination with other countries.</p> <p>B. The attributes can be represented as a data structure (e.g., XML/JSON) and then digitally signed using the private key of the agency. Some of these fields may be password protected/encrypted. (e.g., a unique ID number may be hashed/masked/or replaced with a virtual ID number, and fingerprint should only be used if the storage medium is secure, e.g., on a smartcard).</p> <p>C. This data structure can be encoded in a barcode or represented as an electronic data file (JSON/XML/PDF) and stored on any electronic device.</p> <p>Authentication:</p> <ol style="list-style-type: none"> 1. Person from Country B seeks <i>in-person</i> service in Country A using a credential issued by Country B. 2. Service Provider verifies the credential using the signer (public key) certificate and root certificates which have been previously stored locally. 3. Service provider compares the face image on the credential with that of the person and allows access. Other authentication factors such as password, PIN, etc. may be used for higher assurance transactions. <p><i>Note:</i> transaction logs are uploaded when connectivity is available to the central system. Notification of the authentication even is sent to the user based on user choice (e.g., mobile or email).</p>	<ul style="list-style-type: none"> ▪ Credential issuance ▪ Service providers need to store signer certificates, root certificates, and revocation lists locally (e.g., for ICAO Public Key Directory model or adaptation) ▪ The Identity Provider should keep the private key of the signer digital key pair in secure custody (tamper proof) ▪ The credential should be digitally signed. ▪ The service provider needs to compare the face/biometric of physically present person with that stored on the credential

Box 43. Proposal for mutual recognition of national IDs in the East African Community (EAC)

In 2017 and 2018, the World Bank partnered with the EAC secretariat and six Partner States to carry out a study of what options exist for mutual recognition of national IDs in the EAC, including for migration and for online cross-border transactions. The following roadmap was developed through the consultative process:



- **Milestone 1: National ID System** envisions achievement of a legally-enabled, robust, inclusive, and responsible national ID system. This includes a national ID database that enables electronic authentication of individuals for electronic delivery of services, and the capacity to present a credential for electronic authentication at a service delivery point or for an online service.
- **Milestone 2: Presence-Based Authentication** envisions face-to-face identity authentication at service points through various methods. Cross-border delivery of services would be based on authentication of a user with their national ID at the service delivery point, such as: border crossings; hospitals or schools; and banks.
- **Milestone 3: Presence-Less Authentication** envisions identity authentication for online services from anywhere or from any device based on digital identity. Access to services would be enabled by assurance levels or trust levels through digital identity to open bank accounts, apply for a driver's license, or apply to an educational institution, all online.
- **Milestone 4: Electronic and Digital Signatures** envisions the capacity for online and high assurance transactions from anywhere based on digital identity and electronic and digital signatures. Users would be able to perform transactions which require legally acceptable signatures, such as electronic voting, land purchase transactions, or issuance of online certificates by Government/educational institutions.

Source: Adapted from *Study of Options for Mutual Recognition in East Africa*

STANDARDS

Standards—a set of specifications and procedures with respect to the operation, maintenance, and reliability of materials, products, methods, and services—are the backbone of the technical architecture of the ID system. They establish universally understood and consistent interchange protocols, testing regimes, quality measures, and good practices with regard to the capture, storage, transmission, and use of identity data, as well as the format and features of identity credentials and authentication protocols.

Standards are rigorously defined by organizations who set up, publish, monitor, and continuously update standards to address a range of issues related to ID systems. Standard-setting bodies including **international organizations** (e.g. the International Organization for Standardization or [ISO](#), the International Telecommunication Union or [ITU](#), the International Civil Aviation Organization or [ICAO](#), the International Electrotechnical Commission or [IEC](#), etc.), **regional organizations** such as the European Committee for Standardization ([CEN](#)), and **national organizations** such as the U.S. National Institution of Standards and Technology ([NIST](#)) or the Unique Identification Authority of India ([UIDAI](#)). In addition, a number of **industry consortia and non-profit organizations**—such as the Fast Identity Online ([FIDO](#)) Alliance, Open Identity Exchange ([OIX](#)), and [GSMA's Mobile Connect](#)—are also involved in developing standards.



The choice of standards is essential at each stage of the identity lifecycle, and has implications for:

- Technology and vendor neutrality (see Box 44)
- The accuracy, quality, and consistency of data collection and the security of the system
- The interoperability of the ID system and the mutual recognition of credentials with other systems or jurisdictions
- The level of trust in identities and authentication protocols
- System and information security standards and protocols
- The procurement process

For example, by adopting open standards for an ID system, there is a better chance that it will be able to communicate with other information systems (even if they adopt different standards) and that the software and hardware (and/or an external service provider) could be changed with minimal additional costs and processes. For example, adoption of open standards for raw biometric images (e.g. WSQ or JPEG2000) would allow an ID authority to re-generate templates using a replacement ABIS instead of having to pay fees for images in a proprietary format to be converted into open formats. In some cases, products or services might be offered at a reduced upfront cost provided that the data and technology is proprietary, which could lead to problems in the future when change is required. The outcome of adopting open standards is a reduced long-term cost and greater flexibility, control and ownership.

In particular, this Guide focuses on standards across two categories of standards that are vital for ensuring technology and vendor neutrality, the quality of data collection, and interoperability and mutual recognition:

1. **Technology standards**, which govern the software and hardware components of the ID system and the systems and platforms that enable machine-to-machine communication for interoperability
2. **Data standards**, which govern the format or rules for structuring the data collected by the ID system

Each category of standards is described below, followed by guidance on existing international standards and their implications. For more detailed information, consult the [ID4D Catalog of Technical Standards](#). *Future versions of this Guide will also include more detailed standards for security, including cybersecurity.*

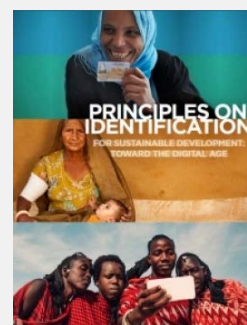
Box 44. Vendor and technology neutrality

The *Principles* highlight the need for open standards to ensure vendor and technology neutrality. A **technology neutral** design is one that approaches the ID system in an output-oriented way instead of requiring specific technologies. A **vendor neutral** design ensures that a sufficient number of vendors are available to implement and improve the system to ensure competition.

Technology and vendor neutral designs limit dependence on specific technologies and vendors, allowing for competition, lower prices and improved system flexibility including for future upgrades or introduction of new features. Conversely, dependency on a particular technology or a particular vendor can result in vendor or technology “lock-in”, which can increase costs and reduce the flexibility of the system to meet a country’s needs as they develop.

Using **open standards** can help ensure that an ID system is interoperable, and technology neutral. However, if the standard is not widely adopted, this may be indicative of a problem and it may be difficult to ensure competition. In some instances, a closed solution may actually offer greater performance than an open standard. If such cases, practitioners should protect against vendor lock-in through good procurement practices and by selecting systems components that support open API standards and allow access to data in portable, open formats (e.g., using data standards). This approach will also enable components to be switched in and out of the ID system over time as vendors change or as new, more efficient solutions are developed. In addition, proprietary standards may be preferred for functions of an ID system that are self-contained and do not require interoperability (e.g., deduplication), assuming vendor lock-in is not a concern.

Source: Adapted from the [ID Enabling Environment Assessment \(IDEEA\)](#).



Technology standards

Technology standards relate to the hardware, software, and platform involved in most technical aspects of the identity lifecycle, including creating and proofing identities, issuing credentials, authentication of identities, and the interoperability with other databases.

Major standards to facilitate the technical quality and interoperability of the ID system related to: (1) **biometrics**, (2) **cards**, (3) **2D barcodes**, (4) **digital signatures**, and (5) **federation protocols**. In some cases, standards represent a clear consensus, and are used by a majority of ID systems globally. In other cases, there are competing standards that countries must adjudicate between. Different standards will also apply depending on the general design and goals of the ID system (e.g., whether the ID card will be used for international travel).

In order to assist practitioners with this process, ID4D has developed a catalog of technical standards, that enumerates existing standards in these five areas and includes a decision tree to clarify where choices need to be made (see Figure 36 below). Readers should consult the full publication for more guidance on adjudicating between applicable standards.

Importantly, standards are not static and will evolve over time as new technologies emerge. Therefore, it is important to stay informed regarding emerging technologies and standards relevant for ID systems. For example, some work-in-progress standards include:

- ISO 29794-part 5: The new expanded standard on facial biometrics, which could go live by 2020.
- ISO/IEC JTC/1 SC/17 SG/2: A special group on standards for virtual identity.
- Digital Travel Credential (DTC): Looks at both policy and technology and is coordinated between ICAO and ISO.

In general, looking toward the future will also help countries avoid investing in a system which may become outdated quickly as better solutions emerge.

Box 45. Examples of standards use

India's Aadhaar ID system relies on a competitive, standards-based ("plug and play") procurement model. Its standard-setting programs rely on standards that promote transparency, accountability, scalability, and technical compliance. These, and real-time quality monitoring, allow flexibility in procurement and competition among vendors, thereby limiting costs (for more details, see Gelb & Clark 2013b).

Estonia issues a smart "ID-Kaart" with has advanced electronic functions that facilitate secure authentication and legally binding digital signatures that may be used for nationwide online services. The e-ID infrastructure is scalable, flexible, interoperable, and standards-based. All certificates issued in association with the ID card scheme conform with European Directive 1999/93/ EC on the use of electronic signatures in electronic contracts within the European Union (EU). The card complies with the *ICAO Doc 9303* travel document standard, and its two one-dimensional bar codes are based on the ISO 15417 standard are used to encode the personal ID number and the document identification number.

The ID-Kaart is a secure credential for accessing public services. To sign a document digitally, a communication model using standardized workflows in the form of a common document format (DigiDoc) has been employed. DigiDoc is based on XML Advanced Electronic Signatures Standard (XAdes), which is a profile of that standard. XAdes defines a format that enables structurally storing data signatures and

security attributes associated with digital signatures and hence caters for common understanding and interoperability.

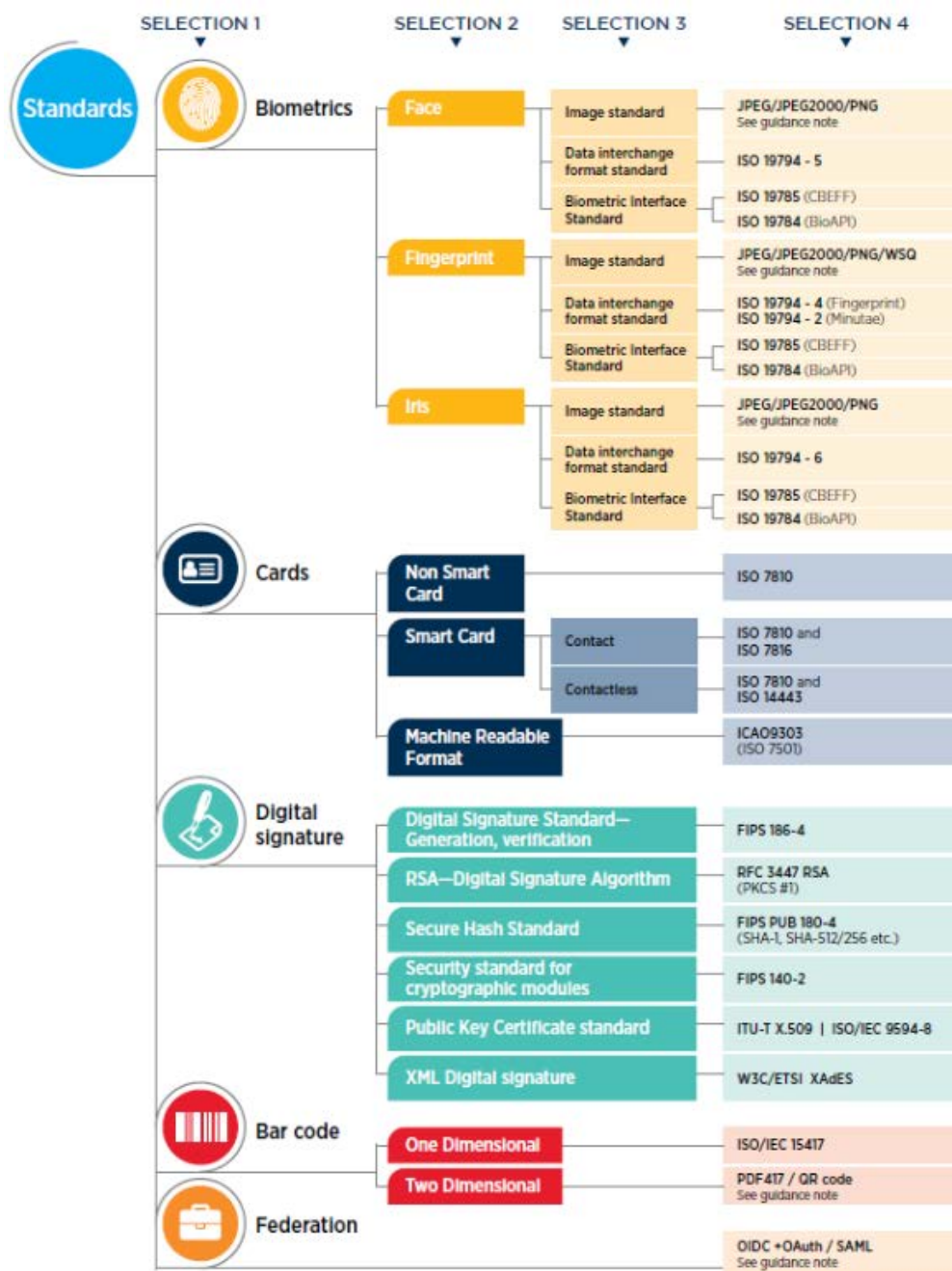
Malawi has recently issued a biometric national ID card that includes an ICAO Identity Applet that will allow card holders to use it for all national travel at airports. In addition, an e-Health Applet that is compliant with European standard CW15974 will would health offices to use the card to verify identity information and authorize the user for services.

Pakistan's National Database and Registration Authority (NADRA) issues a smart National ID Card for Overseas Pakistanis (NICOP) that complies with ICAO standards 9303 (Part 3) and is also ISO 7816-4 compliant. This means that the card can be accepted as a form of digital ID in all international airports and at points of entry and departure.

Peru's National Electronic ID Card (DNle) provides citizens with a digital identity that can be authenticated physically and virtually. The DNle includes two digital certificates that allow the cardholder to sign electronic documents with the same probative value as a handwritten signature. The card complies with the ISO/IEC-7816 standard and its biometrics system followed ISO/IEC 19794. The card is also compliant with ICAO Doc 9303 and can therefore also be used as a machine-readable travel document.

Source: Adapted from the *ID Enabling Environment Assessment (IDEEA)* and *Catalog of Technical Standards*

Figure 36. Technical standards decision tree



Source: Catalog of Technical Standards for Digital Identification Systems. ID4D Initiative, The World Bank.

Data standards

Data standards are **the rules for structuring information collected by the ID system** which facilitate semantic interoperability. A set of agreed-upon data standards ensures that the data entered into a system can be reliably read, sorted, indexed, retrieved, and communicated between systems. Data standards are therefore crucial for ensuring interoperability and the accuracy and portability of identity data, helping protect its long-term value. Data standards can specify, for example:

- Length of a field (e.g., how many characters a name can be)
- Format (e.g., numeric or strings of letters)
- Permissible values (e.g., male, female, other)
- Order of entry (e.g., year, then month, then date)
- Code directories (i.e., standard codes used to abbreviate fields, such as states or provinces)

Table 37. Comparative data standards for India, EU and ICAO

Field	India (Aadhaar)	EU (eIDAS)	ICAO
Name	99-character string	Family name, first name (character string)	Primary identifier, secondary identifier (varies from 39 to 30 characters depending on the form factor of the card/document)
Date of birth	DD/MM/YYYY	YYYY-MM-DD	DD MM YY or DD MM YYYY or DDmonYY, etc. For machine readable zone (MRZ) the format YYMMDD
Address	8 strings (lines) + Pincode	8 strings (lines) + post code	Place of birth—town, city, country, citizenship country code (3) or full name
Gender	M/F/T	Female/Male/Unspecified	M/F/< (unspecified)
ID number	12-digit random number	<issuer country code>/<service provider country code>/< alphanumeric identifier> (e.g., ES/AT/02635542Y, Spanish ID number for an Austrian service provider)	9 character alphanumeric

Table 37 provides some illustrative examples of different standards used by three organizations for attributes such as name and date of birth. Although the particular data standards used will vary by context, it is crucial that identity providers define and enforce an agreed-upon set of data standards by registration agents and any other users able to edit data fields. Such standards will help:

- **Prevent data loss.** The length of data fields (e.g., how many characters you can enter for a person's name) should be standard across database applications. If fields differ by length, it

will be necessary to truncate the data in some cases, which results in loss of data and added computational complexity to define and implement rules for truncation. [Note that ICAO Doc 9303 has detailed standards for truncating names.]

- **Avoid wrong interpretation of data.** Certain attributes (such as first, middle, and family names, or years, months, and days) have a defined order in which they must be captured in order to avoid error and misinterpretation.
- **Promote efficiency and accuracy of data collection and exchange.** Code directories—such as standardized abbreviations or numerical codes for geographic units—help improve the efficiency of data entry and minimize data errors due to misspellings, while improving interoperability with other systems that use the same standards.
- **Facilitate data sharing across systems and borders.** Data standards provide a framework for the interpretation of data shared across the information systems that help avoid loss of data and facilitate translations across systems.

The ID4D-led Data Standards Working Group is in the process of developing more detailed guidance on data standards.

SECTION IV. Resources

 RESOURCES	 ID4D Materials Annotated guide to Id4D data, research, and planning tools	 Other Resources Publications, references, and tools from other organizations	 Glossary Key terms used throughout the Guide
---	--	---	---

This section highlights resources that have informed the content of this Guide and provide more in-depth information on a variety of topics. This includes a summary of key **ID4D publications and tools** categorized by topic, useful materials and **resources from other organizations**, and a **glossary** of important ID-related terms.

Contents:

- [ID4D Tools and Research](#)
- [Other References and Resources](#)
- [ID4D Glossary](#)

ID4D TOOLS AND RESEARCH BY TOPIC

This Guide draws heavily from the following publications and other resources produced by the ID4D Initiative, which can be found at <http://id4d.worldbank.org/>. In order to streamline reading, these materials are referred to throughout the Guide using the short-hand terms indicated in **bold**, rather than their full publication titles.

Measuring the global ID Gap

To understand the scale of the identification challenge, ID4D has undertaken two major data collection efforts to attempt to triangulate the number of people around the world who do not yet have official proof of identity:

- **Global ID4D Dataset:** Using a combination of self-reported figures from country authorities, birth registration rates, and proxy indicators (e.g., voter registration), the 2018 Global ID4D Dataset estimates that approximately 1 billion people lack official proof of identity. For the third annual update, over 40 country authorities provided direct data on the coverage of their foundational ID systems. See <http://id4d.worldbank.org/global-dataset> to explore the data and estimate. Note, however, that this dataset is intended to produce a *global* estimate but does not provide precise trends or country-level estimates. As such, some country-level figures are less reliable than others.
- **Global Findex Survey:** ID4D partnered with the World Bank's Global Findex team to gather data on national ID coverage, use, and barriers to obtaining proof of identity. The ID4D-Findex survey covers 99 countries representing over 70 percent of the world's population. The survey was carried out over the 2017 calendar year, as part of the Gallup World Poll. Approximately 1000 people were surveyed in each country using randomly-selected, nationally representative samples of the non-institutionalized population aged 15 and above. The "Global ID Coverage by the Numbers: Insights from the ID4D-Findex Survey" note synthesizing high-level results, as well as the dataset itself, can be downloaded at <http://id4d.worldbank.org/global-dataset>.

Planning & Design

The ID4D Initiative has produced a number of resources that provide practitioners with expert guidance on the design of ID systems and tools to use during the planning process. This includes:

- **Principles on Identification for Sustainable Development:** The Principles offer a framework for the realization of inclusive and trusted digital identification systems that maximize the benefits of ID systems for sustainable development while mitigating many of the risks. They were developed through a series of in 2017 and have now been endorsed by 25 international organizations, development partners, NGOs, and private sector associations. The Principles are available in English, French, and Spanish and can be downloaded at <http://id4d.worldbank.org/principles>.

- **ID4D Diagnostic:** World Bank country and regional engagement on ID systems frequently begins with a diagnostic exercise to assess existing and planned ID systems. The ID4D Diagnostic methodology—which replaced the previous Identity Management System Analysis or IMSA—was developed in collaboration with governments and development partners and provides a holistic approach to a country’s identity ecosystem, including institutions, technology, laws, policies, and practices related to identification. It is guided by the ten Principles on Identification for Sustainable Development. See <http://id4d.worldbank.org/Diagnostic-Guidelines> for the latest version of the Guidelines (current version released in 2018).
- **ID Enabling Environment Assessment (IDEEA):** The World Bank’s IDEEA tool—released in 2018—is a due diligence questionnaire intended to facilitate a systematic assessment of a country’s existing ID systems alongside an examination of its enabling laws and regulations, and institutions. To ensure that the legal and regulatory review is carried out in context, the IDEEA includes a range of questions about the purpose, design, usage, institutions and cultural context surrounding a country’s national ID and civil registration systems. It is designed to generate a country profile that can be used to identify areas where administrative and legal frameworks might be strengthened to support the development of digital ID (<http://id4d.worldbank.org/legal-assessment>).
- **Technical standards catalog:** “The Catalog of Technical Standards for Digital Identification System” (2018) serves as a reference for practitioners considering which technical standards to adopt during the implementation of an ID system or project. The catalog includes a decision tree and tables that summarize currently available standards provide guidance in cases of competing standards (<http://id4d.worldbank.org/technical-standards>).
- **Costing Study and Model:** Based on a survey of 15 countries, this 2018 costing study analyzes the key country characteristics and program design choices that have a significant impact on the cost of ID system. The accompanying Excel model allows practitioners to estimate the cost of a planned ID system by varying key characteristics, design choices, and assumptions (<http://id4d.worldbank.org/Cost-Model>).
- **Public Sector Savings Report:** “Public Sector Savings and Revenue from Identification Systems: Opportunities and Constraints” (2018) aggregates existing evidence from a variety of countries, to build a framework for analyzing the potential fiscal benefits associated with investment in ID systems, including the features, mechanisms, and conditions that may generate (or limit) savings and revenue. It also provides a tool for governments and other stakeholders involved in planning or funding such systems to begin estimating expected fiscal returns on their investments (<http://pubdocs.worldbank.org/en/745871522848339938/PublicSectorSavingsandRevenueIDSystems-Web.pdf>).
- **Private Sector Savings:** “Private Sector Economic Impacts from Identification Systems” (2018) This paper applies the framework developed in the public-sector savings paper (above) to the private sector, aggregating evidence on how digital ID systems have helped generate revenue and savings for the private sector through multiple channels (<http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSystems-Web.pdf>).

- **Technology Landscape:** “Technology Landscape for Digital Identification” (2018) is a first attempt to develop a comprehensive overview of the current technology landscape for digital ID. It highlights key benefits and challenges associated with each technology, and provides a framework for assessing each technology on multiple criteria, including length of time it has been in use, its ease of integration with legacy and future systems, and its interoperability with other technologies
(<http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf>).
- **Privacy by design:** “Privacy by Design: Current Practices in Estonia, India and Austria” (2018) describes the privacy-by-design approach to protecting personal data and synthesizes some of the specific legal, operational, and technical controls for data protection adopted in three countries, including the use of tokenization, personal access portals, random numbers, minimal data collection, and more.
(<http://documents.worldbank.org/curated/en/546691543847931842/pdf/132633-WP-PrivacyByDesign-112918web.pdf>).
- **Digital Identity Toolkit:** The “Digital Identity Toolkit: A Guide for Stakeholders in Africa” (2014) provides guidance on developing digital ID systems for to meet sustainable development goals, with a focus on Sub-Saharan Africa. Much of the material in this Practitioner’s Guide draws on and updates the information provided in the toolkit.
(<http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa>)
- **Public-private cooperation:** “Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation, A joint World Bank Group–GSMA–Secure Identity Alliance Discussion Paper” (2016) gives an overview of potential models of public and private sector cooperation to provide digital ID systems that further development goals, including key considerations and pre-conditions for successful partnerships.
(<http://documents.worldbank.org/curated/en/600821469220400272/Digital-identity-towards-shared-principles-for-public-and-private-sector-cooperation>).
- **Incentives for birth registration:** Based on a review of evidence from Asia, Africa, and Latin America, “Incentives for Improving Birth Registration Coverage: A Review of the Literature” (2018) describes a framework of supply and demand factors that could affect birth registration rates. It finds that birth registration with social transfer programs, such as cash transfers, has been associated with increased birth registration rates in many countries
(<http://pubdocs.worldbank.org/en/928651518545413868/Incentives-and-Birth-Registration030518.pdf>).
- **Study of Options for Mutual Recognition in East Africa.** This framework identifies various options for the mutual recognition and interoperability of national ID in the East African Community (EAC).
(<http://documents.worldbank.org/curated/en/337501535031584335/pdf/129621-ACS.pdf>).
- **Biometrics guide (forthcoming):** This report will provide an in-depth overview of the use of biometric recognition in digital ID systems. This will include guidance on the proper use of biometrics as defined by international principles and standards; good practices and a checklist for the deployment of biometric ID systems that are fair, accessible, inclusive and

secure while respecting privacy; and an overview of commercially available biometric products and solutions, including capture devices, biometric software, and systems for de-duplication.

- **Cybersecurity note (*forthcoming*):** This Practitioner’s note will highlight important issues and best-practices regarding cybersecurity of ID system, including risk analysis, capacity and skills gap analysis, recommendations, and an action plan to identify the solutions needed to mitigate cybersecurity threats.
- **Disability and ID guidance note (*forthcoming*):** This note will provide practical guidance for practitioners on the successful inclusion of persons with disabilities throughout the identity lifecycle, from communications outreach to the collection of biometrics and implementation of verification/authentication services. Lessons and recommendations will be drawn from national consultations with people with disabilities in Nigeria, Guinea, and Cote d’Ivoire, as well as from the available literature around biometric enrollment of people with disabilities for elections.
- **End-user research toolkit (*pre-publication*):** This toolkit will serve as a resource for practitioners and World Bank task teams to conduct qualitative end-user research as part of the public consultation process during project planning. It will include a methodological overview, best-practices, and questionnaires, instruments, and other tools from previously conducted end-user research on ID.
- **Mass registration note (*pre-publication*):** This note will present lessons learned from countries’ experiences of undertaking mass registration for their foundational ID systems. It will provide guidance for countries embarking on ID programs to determine whether mass registration is the appropriate approach for their context. Case studies from Bolivia, Rwanda, Malawi and Pakistan will be included.
- **Procurement checklist (*pre-publication*):** This Checklist will be a user-friendly tool designed to assist practitioners with the procurement process for ID systems. The Checklist addresses common pitfalls that can lead to vendor lock-in or other issues, which can reduce the performance of an ID system and increase costs.

Role of ID by Sector

In addition to the technical materials described above, a series of ID4D papers conduct an in-depth analysis of the role of identification and authentication in different sectors and issue areas, including:

- **Agriculture:** “The Role of Digital Identification in Agriculture: Emerging Applications” (2018) looks at key applications of identification in agriculture to understand how it can help tackle some of the sector’s critical challenges, remove barriers to agricultural productivity, and enhance farmers’ livelihoods, including through (1) increasing the effectiveness and inclusivity of subsidy programs, (2) enabling formal land and asset registration, and (3) improving data about farmers’ economic activity and needs (<http://documents.worldbank.org/curated/en/655951545382527665/The-Role-of-Digital-Identification-in-Agriculture-Emerging-Applications>).

- **Child marriage:** “The Role of Identification in Ending Child Marriage: Identification for Development” (2016) examines how efforts to achieve legal identity for all, including birth registration, can contribute to ending child marriage. This includes an analysis of the link between child marriage and birth registration, identity documents, and marriage laws and certification processes, and a discussion of the broader policy and institutional framework reforms needed to eliminate child marriage.
<http://documents.worldbank.org/curated/en/130281472492551732/The-role-of-identification-in-ending-child-marriage-Identification-for-Development-ID4D>).
- **Forced displacement:** “Identification in the Context of Forced Displacement” (2016) summarizes the particular identity-related challenges of migrants and refugees who have been forcibly displaced from their homes, both within their country and across borders. This includes the potential for a lack of identity documents to be both a cause and consequence of forced internal and external migration, and the particular identity-related needs of displaced peoples that States and the international community must address.
(<http://documents.worldbank.org/curated/en/375811469772770030/Identification-in-the-context-of-forced-displacement-identification-for-development-ID4D>).
- **Financial Services and inclusion:** The “G20 Digital Identity Onboarding” paper (2018) analyzes the role of a trusted digital identification system in financial sector development, particularly the role it plays in furthering the global financial inclusion commitments. It provides insights and recommendation for country-level implementation in line with Principle 7 of the G20 High-Level Principles for Digital Financial Inclusion developed by the Global Partnership for Financial Inclusion
(https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf).
- **Women’s empowerment:** “The Identification for Development (ID4D) Agenda: Its Potential for Empowering Women and Girls” (2015) draws on case studies and national-level data, this paper examines ID systems through the lens of gender inclusion in specific policy areas, including access to financial services, access to social protection schemes, and voting and elections. The evidence suggests that adult women often face gender-specific barriers in obtaining an ID, sometimes related to inability to obtain core documentation such as birth certificates
(<http://documents.worldbank.org/curated/en/859071468190776482/The-identification-for-development-ID4D-agenda-its-potential-for-empowering-women-and-girls-background-paper>).
- **Health:** “The Role of Digital Identification for Healthcare: The Emerging Use Cases” (2018) discusses the potential use of foundational ID systems and credentials for healthcare and presents examples of use cases in Botswana, Estonia, India, Republic of Korea, and Thailand. It highlights key areas where ID systems can be leveraged to improve healthcare outcomes for patients, providers, and government agencies, and in doing so also reinforce the identification system as a whole
(<http://pubdocs.worldbank.org/en/595741519657604541/DigitalIdentification-HealthcareReportFinal.pdf>).

- **Education (*forthcoming*):** This paper will discuss the role of ID systems in helping governments and schools tackle the challenges of getting children into school, keeping attendance high, and delivering a quality education.
- **Digital economy (*forthcoming*):** This Practitioner’s Note will describe how ID plays a central role in building a digital public platform that can help underpin digital transformation.

Country and Regional Cases

A growing set of ID4D and World Bank materials also provide information and cases studies on existing national-level ID systems across the globe, including:

- **ID4D Diagnostics:** To date, Diagnostics (see planning tools above) have been carried out in more than 30 countries. Publicly available reports include: Botswana, Burkina Faso, Cote D’Ivoire, Ethiopia, Guinea, Kenya, Liberia, Madagascar, Mexico, Morocco, Namibia, Nigeria, Peru, Rwanda, Sierra Leone, Somalia, Uganda, and Zambia. Reports, as they are published, are available at <http://id4d.worldbank.org/country-action/id4d-diagnostics>.
- **State of ID in Africa:** In addition to the long-form ID4D Diagnostics, a report on “The State of Identification Systems in Africa: A Synthesis of Country Assessments” (2017) summarizes core findings from 17 Diagnostics conducted in Africa (see <http://documents.worldbank.org/curated/en/156111493234231522/The-State-of-identification-systems-in-Africa-a-synthesis-of-country-assessments>), while the “The State of Identification Systems in Africa: Country Briefs” report (2017) provides snapshots of ID systems in each Sub-Saharan African country (<http://documents.worldbank.org/curated/en/298651503551191964/The-state-of-identification-systems-in-Africa-country-briefs>).
- **Moldova Case Study:** The “Moldova Mobile ID Case Study” details the implementation of the country’s Mobile eID implementation as part of the country’s overall digital transformation. It highlights the role that mobile ID played in improving e-service delivery in key sectors, and articulates key lessons and success factors, including an innovative public-private partnership model, infrastructure, institutional arrangements, and the legal and regulatory environment (<http://documents.worldbank.org/curated/en/279851545919735993/Moldova-Mobile-ID-Case-Study>).
- **South Africa Case Study:** Using the South African experience, this case study highlights the factors that encourage or impeded the adoption of identification and civil registration systems and their ability to advance financial inclusion, women’s empowerment, targeting of social safety nets, agriculture, universal health coverage, resilience building, shock responsiveness, and energy subsidy reform (<http://documents.worldbank.org/curated/en/315081558706143827/South-Africa-ID-Case-Study>).
- **Argentina Case Study (*pre-publication*):** This case study summarizes Argentina’s experience in modernizing and linking its civil registration and ID systems in order to improve coverage and modernize service delivery.

- **India Aadhaar Case Study (*forthcoming*):** This case study focuses on the design and implementation of the Aadhaar unique ID system in India, highlighting key innovations, including de-linking identification and authentication from nationality, designing Aadhaar as a platform, issuing no physical credentials except for a paper receipt, and developing an ecosystem of third-party enrollment agents.

OTHER REFERENCES AND RESOURCES

The World Bank is part of a growing community of practitioners, international organizations, development partners, foundations, NGOs, researchers, and others working to promote identification for sustainable development and provide relevant standards, recommendations, and resources. These materials—along with other references cited throughout this Guide—are listed in here alphabetically.

ADB. 2007. Legal Identity for Inclusive Development. Philippines: Asian Development Bank. <https://www.adb.org/publications/legal-identity-inclusive-development>.

APEC. 2004. APEC Privacy Framework. Singapore: Asia-Pacific Economic Cooperation Secretariat. http://publications.apec.org/-/media/APEC/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf.

Australian Government. 2019. *Trusted Digital Identity Framework: Attribute Profile*. Australian Government Digital Transformation Authority. <https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-attribute-profile.pdf>

Cao, K. and Jain, A. K. 2015. "Learning Fingerprint Reconstruction: From Minutiae to Image." *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 104-117. <https://ieeexplore.ieee.org/document/6928426>.

Cavoukian, A. 2011. "Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

CIS. 2019. Towards a framework for evaluation of Digital ID, 11 June 2019, Draft for Discussion. Center for Internet and Society, India. <https://cis-india.github.io/digitalid.design/evaluation-framework-01.html>

Chadwick, R. 2014. *The Right to Know and the Right Not to Know: Genetic Privacy and Responsibility*. Cambridge University Press.

Chu, Z., Yuan, G., Zhang, X., and Han, L. 2012. "Fingerprint orientation reconstruction from minutiae points." Proceedings of the 10th World Congress on Intelligent Control and Automation, Beijing, pp. 4583-4587. <https://ieeexplore.ieee.org/document/6359347>.

Council of Europe (CoE). 2018. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+)*. <https://www.coe.int/en/web/data-protection/convention108-and-protocol>.

Danezis, G. et al. 2015. Privacy and Data Protection by Design: From Policy to Engineering. European Union Agency for Network and Information Security (ENISA). <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.

- EC. 2017a.** The New European Interoperability Framework: Promoting seamless services and data flows for European public administrations. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.
- EC. 2017b.** Principles and guidance on eID interoperability for online platforms. eIDAS Observatory.
- EU. 2015.** Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOL_2015_235_R_0002
- EU. 2016.** General Data Protection Regulation 2016/679 (GDPR). <https://gdpr-info.eu>.
- FICAM.** *undated*. Streamline Identity Management Playbook. United States Federal Identity, Credential, and Access Management. https://bnbuckler.github.io/ficam-identity/2_step-2/.
- Gelb, A. and Clark, J. 2013a.** Identification for Development: The Biometrics Revolution, *CGD Working Paper 315*. Washington, DC: Center for Global Development. <https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315>.
- Gelb, A. and Clark, J. 2013b.** Performance Lessons from India's Universal Identification Program. *CGD Policy Paper 020*. <https://www.cgdev.org/publication/performance-lessons-india%E2%80%99s-universal-identification-program>.
- Gelb A., and Diofasi, A. 2018.** *Identification Revolution: Can Digital ID be Harnessed for Development?* Washington, DC: Brookings. <https://www.brookings.edu/book/identification-revolution/>.
- Government of India. 2010.** Guidelines for Usage of Digital Signatures in e-Governance, Version 1.0" (December 2010). Department of Information Technology Ministry of Communications and Information Technology. <http://egovstandards.gov.in/guidelines-0>.
- GSMA. 2019.** Exploring the Gender Gap in Identification. London, UK: GSMA. <https://www.gsma.com/mobilefordevelopment/blog/exploring-the-gender-gap-in-identification-policy-insights-from-10-countries>.
- Harbitz, M. and Kentala, K. 2013.** Dictionary for Civil Registration and Identification. Washington, DC: Inter-American Development Bank. <https://publications.iadb.org/en/dictionary-civil-registration-and-identification>
- ICAO. 2018.** Traveler Identification Program (TRIP) Guide on Evidence of Identity. International Civil Aviation Organization. <https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20Guidance%20on%20Evidence%20of%20Identity.pdf>.

- ICAO Doc 9303:2015.** *Machine Readable Travel Documents*.
<https://www.icao.int/publications/pages/publication.aspx?docnum=9303>.
- IDB. 2011.** Identification and Governance Policies: The Legal, Technical, and Institutional Foundations that Influence the Relations and Interactions of the Citizen with the Government and Society. Washington, DC: inter-American Development Bank.
<https://publications.iadb.org/bitstream/handle/11319/5448/Identification%20and%20Governance%20Policies.pdf?sequence=1>.
- IDinsight. 2018.** *State of Aadhaar Report, 2017-2018*. <https://www.idinsight.org/state-of-aadhaar>.
- ISO/IEC. 2011.** ISO/IEC 24760-1:2011 Information technology — Security techniques — A framework for identity management — Part 1: Terminology and concepts.
<https://www.iso.org/standard/57914.html>
- ISO/IEC. 2011.** ISO/IEC 29100:2011 *Information technology — Security techniques — Privacy framework*. <https://www.iso.org/standard/45123.html>.
- ISO/IEC. 2015.** ISO/IEC 2382:2015 *Information technology — Vocabulary*.
<https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v1:en>.
- ISO/IEC. 2017.** ISO/IEC 2382-37:2017. *Information technology — Vocabulary—Part 37: Biometrics*.
<https://www.iso.org/standard/66693.html>.
- ITU. 2010.** ITU-T X.1252 *Baseline identity management terms and definitions*.
<https://www.itu.int/rec/T-REC-X.1252-201004-I>.
- ITU. 2018.** Digital Identity Roadmap Guide. International Telecommunication Union.
<https://www.itu.int/en/ITU-D/ICT-Applications/Pages/digital-identity.aspx>
- Joon Song, H et al. 2016.** Korea: An integrated system of civil registration and vital statistics. Washington, DC: World Bank Group.
<http://documents.worldbank.org/curated/en/702081495191844901/Korea-an-integrated-system-of-civil-registration-and-vital-statistics>.
- Kelly, M. and Satola, D. 2017.** “The Right to Be Forgotten.” University of Illinois Law Review, Vol. 1.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2965685
- Kindt, E.J. 2013.** “Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis.” *Springer Science & Business Media*, 2013.
- Kuner, C. and Marelli, M eds. 2017.** Handbook on Data Protection in Humanitarian Action. Switzerland: International Committee of the Red Cross (ICRC).
https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html?__store=default.
- Malik, T. 2018.** Malawi’s Journey Towards Transformation: Lessons from its National ID Project. Washington, DC: Center for Global Development.

<https://www.cgdev.org/publication/malawis-journey-towards-transformation-lessons-its-national-id-project>.

NIST. 2015. Measuring Strength of Identity Proofing. Workshop: Applying Measurement Science to the Identity Ecosystem Version: 1, December 16, 2015.

<https://www.nist.gov/sites/default/files/nstic-strength-identity-proofing-discussion-draft.pdf>.

NIST. 2017. SP 800-63:2017 *Digital Identity Guidelines*. <https://pages.nist.gov/800-63-3/>.

Nyst, C., Pannifer, S., Whitley, E., Makin, P. 2016. Digital Identity: Issue Analysis. Consult Hyperion. https://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf

OECD. 2013. *The OECD Privacy Framework*.

https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD. 2018. *Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers*.

<https://www.oecd.org/internet/consumer/toolkit-for-protecting-digital-consumers.pdf>.

Open Society Justice Initiative and Namati. 2018. A Community-Based Practitioner's Guide: Documenting Citizenship & Other Forms of Legal Identity. Washington, DC and New York, New York: Open Society Foundations and Namati.

<https://www.opensocietyfoundations.org/publications/community-based-practitioner-s-guide-documenting-citizenship-and-other-forms-legal>.

OpenCRVS (open-source digital CRVS solution developed by Plan International).

<https://www.opencrvs.org/>.

OpenID. <https://openid.net/connect/>.

OWI. 2017. "Don't Believe the (Blockchain) Hype: The Definitive Primer on Identity and Blockchain." One World Identity Labs. www.oneworldidentity.com.

OSCE/ODIHR. 2009. Guidelines on Population Registration. Warsaw: Organization for Security and Co-operation in Europe's Office for Democratic Institutions and Human Rights (ODIHR).

<https://www.osce.org/odihr/39496>.

Perrin et al. 2015. *Government Information Sharing Is Data Going Out of the Silos, Into the Mines?* Independent research report commissioned by the Office of the Information and Privacy Commissioner of Alberta, Canada, Digital Discretion Inc.

http://www.oipc.ab.ca/media/389571/Report_Government_Information_Sharing_Jan2015.pdf.

Plan International. 2015. *Civil Registration and Vital Statistics Digitization Guidebook*.

<http://www.crvs-dgb.org/en/>.

Rakgoasi, S.D. et al. 2015. Botswana – Integration of Civil Registration and Vital Statistics and Identity Management Systems: Botswana Success Story. Washington, DC: World Bank Group. <http://documents.worldbank.org/curated/en/963541495179518711/Botswana->

[Integration-of-civil-registration-and-vital-statistics-and-identity-management-systems-Botswana-success-story.](#)

Shepherdson, Kevin et al. 2016. *88 Privacy Breaches to Be Aware Of: Practical Data Protection Tips from Real-Life Experiences*. Singapore: Marshall Cavendish International (Asia).

UC Berkeley. Privacy Patterns. <https://privacypatterns.org/>.

UN. 1988. International Covenant on Civil and Political Rights, General Comment 16 on Article 17. United Nations Office of the High Commissioner on Human Rights. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6624&Lang=en.

UNCITRAL. 2002. *Model Law on Electronic Signatures with Guide to Enactment 2001*. New York: United Nations. <https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/ml-elecsig-e.pdf>

UNDESA. 2014. *Principles and Recommendations for a Vital Statistics System, Revision 3*. New York, NY: United Nations Department of Economic and Social Affairs, Statistics Division. <https://www.un.org/development/desa/capacity-development/tools/tool/principles-and-recommendations-for-a-vital-statistics-system-revision-3/>.

UNHCR. 2003. *Handbook for Registration: Procedures and Standards for Registration, Population Data Management and Documentation*. United National High Commissioner for Refugees. <https://www.refworld.org/pdfid/3f967dc14.pdf>.

UNICEF. 2017. Birth Registration Estimates (Data). <https://data.unicef.org/topic/child-protection/birth-registration/>.

WEF. 2016. Blueprint for Digital Identity. World Economic Forum. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

World Bank. 2016a. Cloud Readiness Pilot Assessment Report. Washington, DC: World Bank. <http://documents.worldbank.org/curated/en/268981494409143827/Cloud-readiness-pilot-assessment-report>.

World Bank. 2016b. World Development Report 2016: Digital Dividends. Washington, DC: World Bank Group. <http://www.worldbank.org/en/publication/wdr2016>

World Bank. 2017. Toolkit on Combatting Cybercrime. <http://www.combattingcybercrime.org/>.

World Bank. 2018. Civil Registration and Vital Statistics e-learning (developed in collaboration with the Global CRVS Group). <https://olc.worldbank.org/content/civil-registration-and-vital-statistics-systems-basic-level-self-paced-format>.

World Bank and United Nations. 2017. Combatting Cybercrime: Tools and Capacity Building for Emerging Economies, Washington, DC: World Bank Group. <http://documents.worldbank.org/curated/en/355401535144740611/Combatting-Cybercrime-Tools-and-Capacity-Building-for-Emerging-Economies>.

- World Bank and World Health Organization (WHO). 2015.** Global CRVS Scaling Up Investment Plan 2015-2024. Washington, DC: World Bank Group.
<http://www.worldbank.org/en/topic/health/publication/global-civil-registration-vital-statistics-scaling-up-investment>.
- Whitley, E. A. 2018.** Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach. *Center for Global Development*. <https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach>.
- Whitley, E. A., and Hosein, G. 2010.** Global Identity Policies and Technology: Do we Understand the Question?. *Global Policy* 1(2), pp. 209–215.
- WHO. 2013.** Resource Kit on strengthening CRVS for births, deaths and causes of death. Luxembourg: World Health Organization.
https://apps.who.int/iris/bitstream/handle/10665/78917/9789241504591_eng.pdf;jsessionid=76F69E8009ECECBDD8616E66567F1770?sequence=1.

GLOSSARY

This glossary provides operational definitions of identity-related concepts as commonly used in the development sector. They are part of an effort by the World Bank to standardize the language we use in ID4D publications and operational work, and we hope they will be useful to other development partners and practitioners as a point of departure.

Attribute

A named quality or characteristic inherent in or ascribed to someone or something (adapted from *NIST 800-63:2017*). In ID systems, common identity attributes include name, age, sex, place of birth, address, fingerprints, photo, signature, identity number, etc.

Authentication

The process of establishing confidence that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more “factors” to “assert” their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints) (adapted from *NIST 800-63:2017* and *OWI 2017*).

Usage:

- “Two-factor” authentication involves more than one of the factors describes above (i.e., two things that you are, know, or have).
- Although authentication and verification are related and often used interchangeably, for the purposes of this Guide they can be distinguished by whether the process involves determining the veracity of particular attributes (verification) or ensuring that a person is the “true” owner of an identity or credential (authentication). In some cases, however, authentication procedures go beyond establishing a legitimate claim to an identity and also verify particular attributes.

Authoritative source

An authoritative source of identity information is a repository or system that contains attributes about an individual and is considered to be the primary or most reliable source for this information. In the case that two or more systems have mismatched or have conflicting data, the data within the authoritative data source is considered the most accurate (*FICAM, undated*).

Authorization

The process of determining what actions may be performed or services accessed on the basis of the asserted and authenticated identity (*Nyst et al. 2016*).

The granting of rights and, based on these rights, the granting of access (*ITU-T X.1252*).

Biographic data

For the purpose of this Guide, biographic data refers to attributes about a person or their life, that are not biometric (i.e., biological or behavioral). In foundational or legal ID systems, this often includes information such as name, sex, age, nationality, etc.

Usage:

- Although often used interchangeably with “**demographic**,” the term “biographic” is preferred when referring to personal data—i.e., information about a person or their life. The term “demographic” is more appropriate when discussing the statistical characteristics of a population or a subgroup (e.g., categorizing the population by sex, age, income group, etc.).

Biometric characteristic

A biological (fingerprint, face, iris) or behavioral (gait, handwriting, signature, keystrokes) attribute of an individual that can be used for biometric recognition (adapted from *ISO/IEC 2382-37*).

Biometric identification

The process of searching against a biometric enrollment database to find and return the biometric reference identifier(s) attributable to a single individual (*ISO/IEC 2382-37*). Biometric identification is often used to deduplicate identity records during registration (i.e., to perform a duplicate biometric enrollment check).

Biometric recognition

The automated recognition of individuals based on their biological and behavioral characteristics. Biometric recognition encompasses both biometric identification and biometric verification (*ISO/IEC 2382-37*).

Biometric verification

The process of confirming a biometric claim through biometric comparison (*ISO/IEC 2382-37*). Biometric verification may be used during authentication procedures to conduct a 1:1 match of a captured biometric template (i.e., the biometric claim) against one stored on a card, mobile device, or database.

Civil registration

The continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population, as provided through decree or regulation in accordance with the legal requirements of each country (*UNDESA 2014*). Vital events concern the life, death and civil status of individuals, including live birth, death, fetal death, marriage, divorce, separation, annulment, adoption, legitimation, and recognition (of paternity).

Credential

A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider (adapted from *ID4D Technology Landscape* and *Public-Private Cooperation* reports).

Usage:

- Identity “credential” is preferred to identity “document” in most contexts as many digital credentials are not physical documents.

Cybercrime

Cybercrime is understood to include criminal conduct (as provided in the country’s criminal laws) directed against the confidentiality, integrity and availability of computer systems and networks, as well as the data stored and processed on them, and criminal acts carried out through the instrumentality of such systems, networks and data (*World Bank & United Nations 2017*).

Cybersecurity

The term “cybersecurity” is a convenient shorthand for a complex set of issues. It commonly refers to systems and actions aimed at securing data and communications over the internet and even the infrastructure of the internet itself. includes “cybercrime.” The more common threats to cybersecurity are malware, denial of service, and phishing attacks (attempts to acquire sensitive information online by someone who is masquerading as a trusted entity), but cyberincidents are increasingly perpetrated by disaffected insiders. cybersecurity usually refers to securing data and infrastructure in a civilian context; but acts that might previously have been considered civilian attacks are now being uncovered as acts of states against states via nonstate actor proxies, blurring the lines between acts of cybercrime and cyberwar or cyberterrorism (*World Bank 2016b*, p. 222).

Deduplication

In the context of identification systems, deduplication is a technique to detect duplicate identity records, identify inconsistent identity claims, and establish the uniqueness of people within a system. Biometric recognition is commonly used to perform this function; biographic data can also be used for deduplication but generally not with the same level of efficiency nor accuracy (adapted from *ISO/IEC 2382-37* and *ID4D Technology Landscape report*).

Derived credential

A credential issued based on proof of possession and control of an authenticator associated with a previously issued credential, so as not to duplicate the identity proofing process (*NIST 800-63:2017*).

Digital identity

A set of electronically captured and stored attributes and/or credentials that uniquely identify a person (adapted from *Harbitz & Kentala 2013* and *ID4D Technology Landscape report*).

Usage:

- Use “digital identity” when referring to a person’s digital identity, and “digital ID” when referring to a digital identity credential or system.

Digital identification (ID) system

An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication (adapted from *ID4D Public-Private Cooperation* report).

Digital signature

An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection (*NIST 800-63:2017*).

Usage:

- Note that “electronic signature” and “digital signature” are often used interchangeably but are NOT synonymous. Digital signatures are one technical implementation of an electronic signature using public-key cryptography. In addition, digital signatures are also used for other functions (e.g., authenticating devices) that do not serve the same purpose as an electronic signature, which is to substitute for a handwritten signature.

Electronic signature

An electronic authentication technique that carries the legal weight of—and substitutes for—a handwritten signature (adapted from *UNCITRAL 2002*).

Usage:

- Note that “electronic signature” and “digital signature” are often used interchangeably but are NOT synonymous. Digital signatures are one technical implementation of an electronic signature using public-key cryptography. In addition, digital signatures are also used for functions (e.g., authenticating devices) that do not serve the same purpose as an electronic signature, which is to substitute for a handwritten signature.

Foundational identification (ID) system

An identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. Common types of foundational ID systems include civil registries,

universal resident or national ID systems, and population registers (adapted from *Gelb & Clark 2013a* and various ID4D publications).

Usage:

- Countries typically have multiple foundational ID systems that may or may not be entirely distinct. For example, a country may have a population register linked to the civil registration system that is used both to generate population statistics and as the basis on which national ID cards are issued.
- Foundational ID systems are also typically legal ID systems, with the primary purposes of establishing or recognizing legal identity and issuing government-recognized credentials.
- The distinction between foundational and functional ID systems is about the *purpose* for which they were created. In some countries—typically where foundational ID systems have been weak or non-existent outside of civil registration—functional credentials are used as the primary means of identification and authentication for a variety of purposes, (e.g., driver’s licenses or social security numbers in the U.S.); however there are not typically considered to be foundational systems as their primary purpose is still sector-specific.

Functional identification (ID) system

An identification system created to manage identification, authentication, and authorization for a particular service or transaction, such as voting, tax administration, social programs and transfers, financial services, and more. Functional identity credentials—such as voter IDs, health and insurance records, tax ID numbers, ration cards, driver’s licenses, etc.—may be commonly accepted as proof of identity for broader purposes outside of their original intent, particularly when there is no foundational ID system (adapted from *Gelb & Clark 2013a* and various ID4D publications).

ID

- Identity document (see credential).
- See identification.

Usage:

- Use “identify” when referring to the verb (e.g., write “people have no way to identify themselves” rather than “people have no way to ID themselves”).
- When referring to a specific credential, add a description of that credential after ID whenever appropriate to avoid ambiguity in meaning (e.g., “national ID card” rather than “national ID”).

Identification

The process of establishing, determining, or recognizing a person’s identity (adapted from *ISO/IEC 24760-1:2011* and *ITU-T X.1252*),

Usage:

- Use “identification (ID) system” when referring to the specific processes or systems used for identification.
- Use “identity document,” “ID,” or “credential” when referring to a “form of identification”

Identification (ID) system

The databases, processes, technology, infrastructure, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose (adapted from the *Principles on Identification*).

Usage:

- “identification (ID) system” is generally preferred over “identity system,” including in all compound types of ID systems (e.g., use “foundational *identification/ID* system” rather than “foundational *identity* system”).

Identity

A set of attributes that uniquely describe a person within a given context (adapted from *NIST 800-63:2017*).

Identity document (ID)

A type of identity credential. See also ID.

Identity ecosystem

The set of identification systems—including databases, credentials, laws, processes, protocols, etc.—and their interconnections within a jurisdiction, geographic area, or particular sector (adapted from *ID4D Public-Private Cooperation* paper).

Identity lifecycle

The process of registering, issuing, using and managing personal identities, including collecting identity data; validation through identity proofing and deduplication; issuing credentials; verification and authentication for transactions; and updating and/or revoking identities and credentials (adapted from *ID4D Public-Private Cooperation* paper).

Identity proofing

Establishes the uniqueness and validity of an individual’s identity when they register in an ID system. Identity proofing may rely upon various factors such as identity documents, biographic information, biometric information, and knowledge of personally relevant information or events, and may be done in-person or remotely (adapted from *NIST 2015* and *NIST 800-63:2017*).

Identity provider

An entity—e.g., a government agency or private firm—that issues and manages identities, credentials, and authentication processes throughout the identity lifecycle (*ID4D Public-Private Cooperation* paper).

Usage:

- The terms “identity provider (IdP),” “identity service provider,” and “digital identity service provider” are often used somewhat synonymously in different publications and standards, and are often broken down into more specific roles such as a “registration authority,” “credential service provider,” “attribute provider,” “verifier,” etc., depending on the architecture of the ID system and the various entities and roles involved (e.g., see *NIST 800-63:2017*, *ISO/IEC 24760-1:2011* and *ITU-T X.1252*). In this Guide, the term is used in a generic sense to encompass all or most of these roles unless otherwise stated.

Interoperability

The ability of different functional units—e.g., systems, databases, devices, or applications—to communicate, execute programs, or transfer data in a manner than requires the user to have little or no knowledge of those functional units (adapted from ISO/IEC 2382:2015).

Level of assurance (LOA)

The ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant’s “true” identity (*ID4D Public-Private Cooperation*). The overall level of assurance is a function of the degree of confidence that the applicant’s claimed identity is their real identity (the identity assurance level or IAL), the strength of the authentication process (authentication assurance level or AAL), and—if using a federated identity—the assertion protocol used by the federation to communicate authentication and attribute information (federation assurance level or FAL) (adapted from *NIST 800-63:2017*).

National identification (ID) system

A foundational identification system that provides national IDs (NIDs)—often a card—and potentially other credentials. In many countries, a primary function of national ID systems has been to establish and provide recognition and proof of nationality and/or residency status.

Usage:

- There is no commonly agreed-upon definition of an NID system and countries have used this term to refer to a variety of types of ID systems. For example, “national” may be interpreted both as providing proof of nationality and/or in the sense that the system is nation-wide in scope.
- Most so-called NID systems normally provide proof of legal identity

- Use “national ID” or “NID” when referring to the credential (e.g., a card) and “national ID system” or “NID system” when referring to the entire system, including databases, etc.

Public Key Infrastructure (PKI)

A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates (*NIST 800-63:2017*).

Population register

A database of every individual that has the right to reside in the country, including citizens and non-citizens, children and adults. Population registers typically contain demographic data and life-event information that is the basis of or exchanged with other identification systems and databases such as national ID systems, civil registers, and others (adapted from *Harbitz & Kentala 2013*).

Proof of legal identity

A credential, such as a birth certificate, identity card or digital identity credential, that is recognized as proof of legal identity under national law and in accordance with emerging international norms and principles (United Nations Legal Identity Expert Group Operational Definition of Legal Identity).

Registration

The process through which a person applies for an ID system and the ID provider proofs their identity (adapted from *NIST 800-63:2017*).

- In this Guide, the term “registration” is used interchangeably with “enrollment,” following NIST definitions. Note that other sources have defined these two terms to mean distinct processes (e.g., see *ISO/IEC 24760-1:2011* and *ITU-T X.1252*).

Relying party (RP)

An entity that relies upon the credentials and authentication mechanisms provided by an ID system, typically to process a transaction or grant access to information or a to system (adapted from *NIST 800-63:2017*).

Seeding

One-to-one mapping of identity records in an existing database with those in another database (e.g., via a unique ID number). Seeding can be done in bulk with no action required by individual users (“inorganic seeding”) or on a case-by-case bases as users interact with one of the systems (“organic seeding”) [adapted from ID4D *Aadhaar Case Study (forthcoming)*].

Social register

A database that contains socioeconomic data on the population—at the individual and/or household level—for the purpose of unifying the targeting and distribution of social programs, such as cash transfers and pensions.

Unique ID number (UIN)

In the context of identification systems, a number that uniquely identifies a person—i.e., each person only has one UIN and no two people share the same UIN. UINs are generally assigned for a person's lifetime in a particular ID system (i.e., their number does not change over time), typically after validating a person's identity and uniqueness through deduplication process (adapted from *ID4D Public-Private Cooperation*).

Usage:

- In general, use “UIN” and not “UID” unless referring to a country-specific system (e.g., as in India)
- Many countries have UINs that are referred to as national ID numbers or “NINs”

Universal resident ID system

A digital, foundational ID system that uniquely identifies and provides government-recognized credentials to all residents of a country, including nationals and non-nationals.

Usage:

- NID systems may be universal resident ID systems to the extent that they are digital and provide IDs to residents as well as nationals.

Verification

For the purpose of this document, verification is defined as the process of verifying specific identity attributes or determining the authenticity of credentials in order to facilitate authorization for a particular service.

Usage:

- Although authentication and verification are related and often used interchangeably, they can be distinguished by whether the process involves determining the veracity of specific attributes or credentials (verification) or ensuring that a person is who they claim to be (authentication)
- Note that during the identity proofing process, the term verification is typically used to refer to the process of verifying that the applicant is the true owner of the claimed identity and evidence (i.e., authentication).

id4d.worldbank.org