DRAFT FOR CONSULTATION

PROCUREMENT GUIDE AND CHECKLIST

for Digital Identification Systems

ID4D IDENTIFICATION FOR DEVELOPMENT

WORLD BANK GROUP

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

TABLE OF CONTENTS

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

ABOUT ID4D

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

The mission of ID4D is to enable all people to access services and exercise their rights enabled by inclusive and trusted digital identification systems. 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 responsible digital identification systems that are integrated with civil registration.

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

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

ACKNOWLEDGEMENTS

This guide and checklist were prepared by Ernst & Young Global Limited (Thampy Koshy, Neeraj Jain, Rajeesh Menon and Mohit Singhal), as part of the Identification for Development (ID4D) Initiative, the World Bank Group's cross-sectoral effort to support progress toward identification systems using 21st century solutions. It was made possible through the generous support of the partners of the ID4D Multi-Donor Trust Fund (Bill & Melinda Gates Foundation, the U.K. government, the French Government, the Australian government and the Omidyar Network).

The guide and checklist benefited greatly from the inputs by Seth Ayers, Jerome Buchler, Luda Bujoreanu, Hunt La Cascia, Julia Clark, Adam Cooper, S.M. Quamrul Hasan, Anita Mittal, Georg Neumann, Tiago Carneiro Peixoto, Michiel van der Veen and Edgar Whitley under the supervision of Vyjayanti Desai.

The guide and checklist are being published for consultation and may be updated based on feedback received. ID4D appreciates any feedback by email: id4d@worldbank.org.

ABBREVIATIONS

ABIS	Automated Biometric Identification System
ACD	Automatic Call Distribution
AFIS	Automated Fingerprint Identification System
AMC	Annual Maintenance Contract
API	Application Programming Interface
BOOT	Build Own Operate Transfer
BOT	Build Operate Transfer
COTS	Commercial Off-the-Shelf
CRM	Customer Relationship Management
CRVS	Civil Registration and Vital Statistics
DC LAN	Data Center – Local Area Network
DC WAN	Data Center – Wide Area Network
eID	Electronic Identity
e-KYC	electronic - Know Your Customer
EOI	Expression of Interest
FMR	False Match Rate
FNMR	False Negative Match Rate
FPIR	False Positive Identification Rate
FNIR	False Negative Identification Rate
ICT	Information and Communications Technology
ID	Identity
ID4D	Identification for Development (World Bank Group Initiative)
IEC	Information, Education and Communication
IPR	Intellectual Property Rights
IT	Information Technology
IVRS	Interactive Voice Response System
KPIs	Key Performance Indicators
LOAs	Level(s) of Assurance
MSA	Master Services Agreement
NDA	Non-Disclosure Agreement
NOC	Network Operation Center
OTP	One Time Password
PIN	Personal Information Number
PKI	Public Key Infrastructure
PoA	Proof of Address
PoI	Proof of Identity

PoR	Proof of Residence
RFI	Request for Information
RFP	Request for Proposal
SDG	Sustainable Development Goal
SLA	Service Level Agreement
SOC	Software Operation Center
SOP	Standard Operating Process
UAT	User Acceptance Testing
UIN	Unique Identity Number
YoY	Year on Year

EXECUTIVE SUMMARY

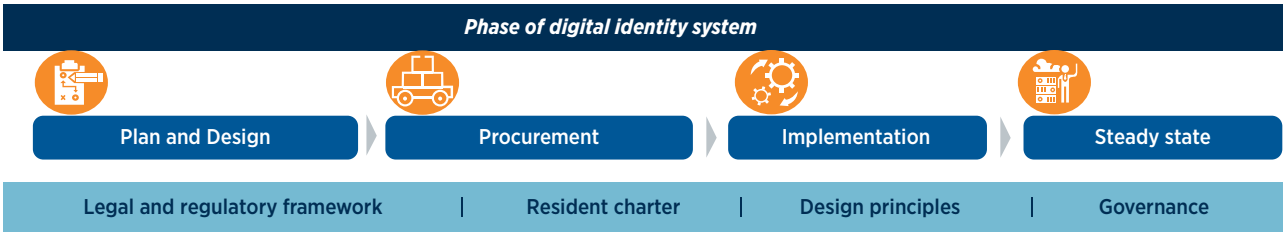
Identity (ID) systems are enablers for countries to achieve economic growth, financial inclusion, and social protection goals. A well-established, foundational ID system can improve efficiency and efficacy of public services delivery and reduce leakages. An estimated one billion people worldwide[1] struggle to prove their identity. The 'invisible billion' are typically members of the poorest and most vulnerable groups, with a majority living in Sub-Saharan Africa and South Asia. Additionally, 47 percent of those without identification (ID) are children or youth under the national ID age who were not registered at birth.

Lifecycle of an ID system: The typical implementation lifecycle of ID systems is illustrated in figure 0.1.

- Plan and Design phase: As a first step, major elements of the ID system are defined. These include big-picture policy decisions, various core and ancillary identity functions, definition of business and operating model(s), transition strategy and institutional structure for managing the program. These are often done within a constitutionally approved legal framework that governs the operation of the program within a country, a resident's charter that drives the goal of people-centricity in the ID services offered by the program, and the design principles for the implementation of the ID system.
- Procurement phase: Once the program strategy for the ID system is defined by the ID authorities in the plan and design phase, the next critical steps are development of procurement strategy and request for proposals (RFP) to select vendors.
- Implementation phase: After the selected vendor(s) are onboarded, implementation activities are initiated. As part of this phase, the ID authority continuously monitor the implementation to ensure that it complies with the requirements.
- Steady state: After a successful deployment of the ID system, the ID authority needs to continuously monitor the performance of the system and the vendor, user experience, and the changes taking place in the ecosystem to ensure sustainability of the program. This will drive refinements, upgrades, and innovations to ensure better performance and user experience.

Importance of Effective Procurement Strategies in Ensuring the Success of an ID system: Implementing ID systems is a challenging endeavor and requires a variety of technological, program, and change management skills, that may need to be sourced from a number of qualified local and global vendors. Often, ill-equipped institutional structures and skill/competency gaps in the local population are challenges faced by low- and middle-income countries in successfully implementing large and complex e-governance programs, like a foundational ID system. Poor procurement processes and weak vendor contract management often leads to failed procurement, implementation delays, and vendor and technology lock-in. A World Bank multi-country study of ID system costs has demonstrated that the impact of procurement strategies could range anywhere between 25 percent to 100 percent of the total cost of the program.[2] Hence, how well the procurement

FIGURE 0.1 Phases of a Digital Identity System



[1] https://id4d.worldbank.org/global-dataset

[2] http://id4d.worldbank.org/Cost-Model.

process is managed is a key determinant of the success of any ID system.

The World Bank published a *Practitioner's Guide*[3] to assist governments, development partners, academics, researchers, and implementation agencies in evaluation, design, implementation, and management of a foundational ID system. This guide provides a 360-degree view of the planning and design phase in greater detail, and practitioners are encouraged to refer to this material for more detailed guidance on high-level policy and design decisions.

Need for a Procurement Guide and Checklist: On account of the complexity and the vastness of diverse procurement practices in digital ID systems across the world, this *Procurement Guidance and Checklist for Digital Identification Systems* has been developed building on the lessons from different countries. It focuses on the procurement phase in greater depth and detail. This document has been designed to be equally useful for countries planning for an entirely new ID system (i.e. a greenfield ID system) as well as for countries that are planning to modernize legacy ID systems (i.e. a brownfield ID system). This document is aimed at assisting governments, multilateral institutions, and consultants in systematically assessing the procurement needs and carrying out the procurement processes in a structured manner.

It is recommended that this document be read along with the reference documents mentioned in this report, and in particular, the *Practitioner's Guide*[4].

The key objectives of this procurement guidance and checklist are to:

- Assist ID authorities and practitioners in outlining a robust ID system procurement strategy.
- Provide guidance on key program decisions and considerations for the development of RFP(s).
- Enable ID authorities in developing effective RFP(s) which are aligned to the short- and long- terms goals of the country, as well as sufficiently elaborating the various business and technical requirements for an ID system.
- Provide a checklist to ascertain whether the ID authorities have accommodated all the necessary considerations around the various design components of an ID system.
- Provide specific guidance around various design and procurement elements in a robust, open, interoperable, technology neutral ID system.
- Highlight the risks of vendor and technology lock-in and the possible mitigation measures.

The procurement phase of an ID system implementation has two key stages – beginning with the development of a procurement strategy, and followed by the procurement process, which includes development of RFPs, bid evaluation and selection of the vendor, and signing of the contract(s) with the selected vendors.

Development of a Procurement Strategy: This requires a detailed assessment of a country's existing ID system(s), current coverage of its population and the target state to be achieved, its current human resource capabilities and institutional structure. Further, a study of the technology landscape is needed to select the system architecture and technologies that are suitable, as well as scanning domestic and international markets to identify potential bidders who have proven capability in executing such large transformation programs. This stage could also involve extensive vendor consultations to gauge market interest. This should form the basis for ID authorities to design an RFP in accordance with its vision that has been developed as part of the plan and design phase.

The procurement strategy should outline the effective approach to bring the various solutions and capabilities together in a holistic fashion and also articulate the nature of engagement between the ID authorities and the various vendors. ID authorities should look to accommodate international best practices and global lessons in their procurement strategies.

Figure 0.2 highlights some of the good procurement practices seen in global ID system implementations.

[3] https://id4d.worldbank.org/guide.

[4] http://id4d.worldbank.org/guide.

FIGURE 0.2 Good Practices for Procurement of ID Systems

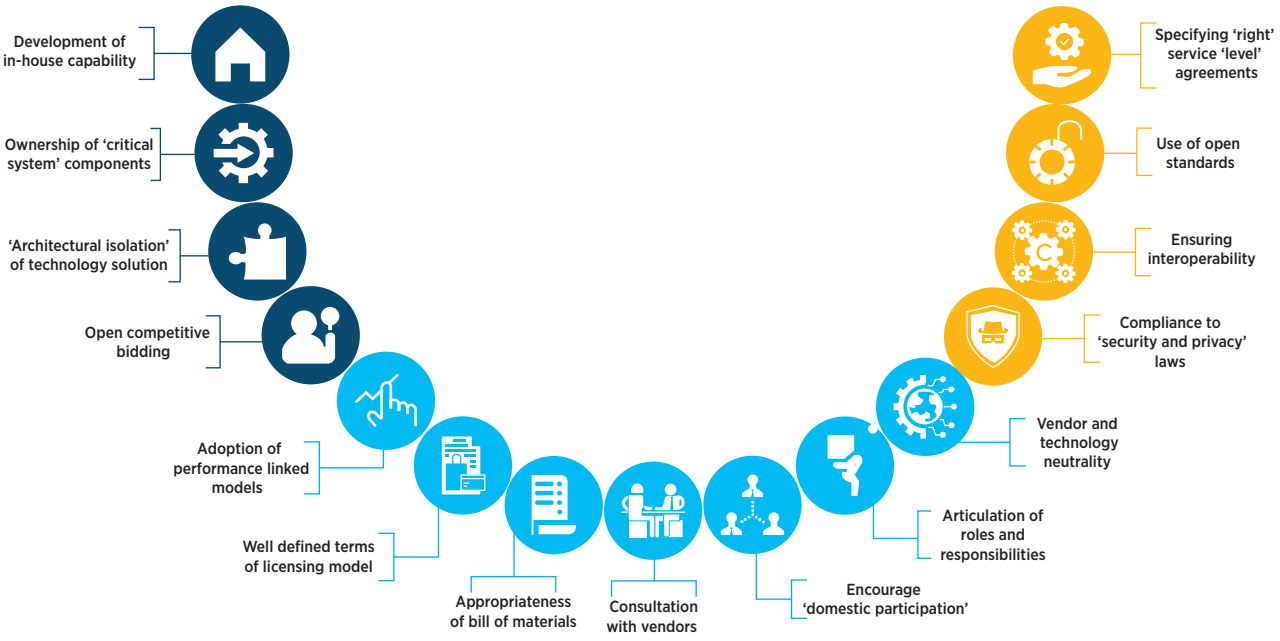
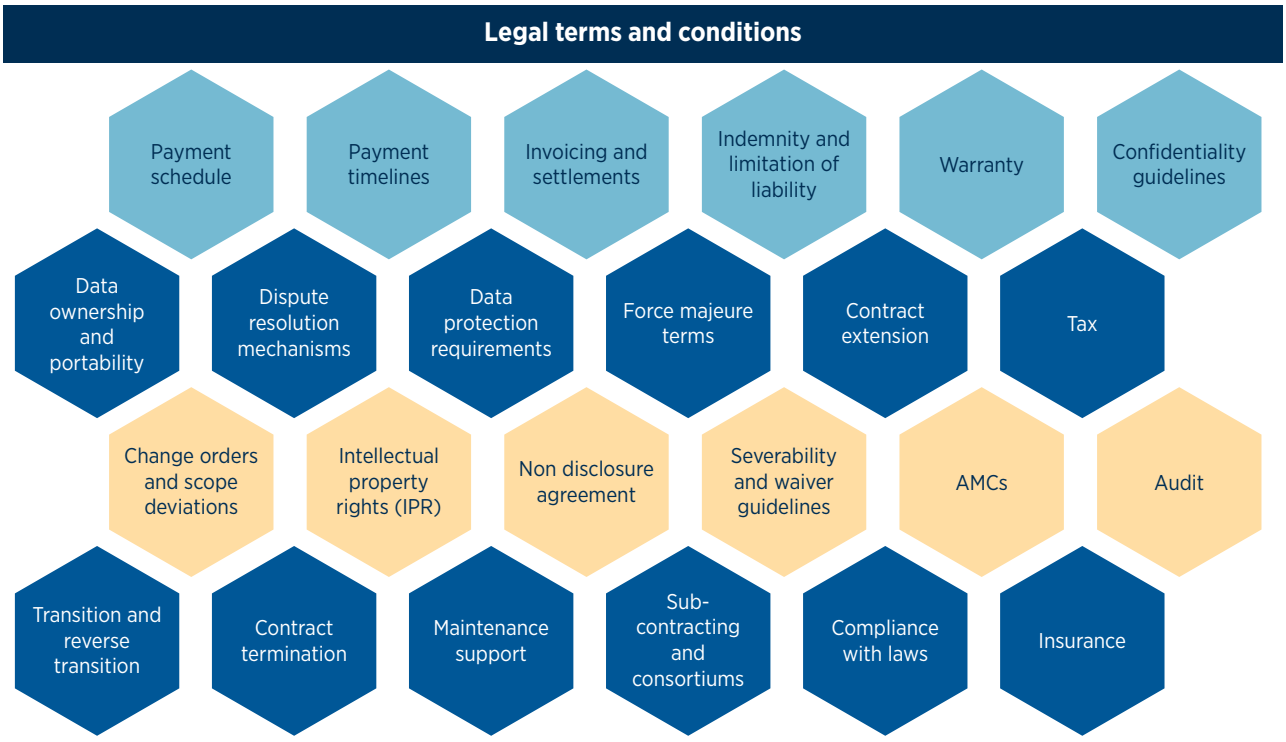


FIGURE 0.3 Legal Terms and Conditions



A key challenge that needs to be tackled while developing the procurement strategy is the potential for vendor lock-in. Therefore, while developing the procurement strategy for an ID system, ID authorities should try to mitigate the risks of vendor and technology lock-in scenarios by using open technology standards, globally accepted interoperability practices, and strong procurement processes that minimize contractual constraints in the choice of technology and supplier(s).

Procurement Process: The development of RFP(s) will be based on the procurement strategy and detailed business/technical specifications designed by the ID authorities (in the plan and design phase, as outlined earlier). The final stage is the conduct of the bid process, followed by the selection of the vendor(s) and awarding of contract(s).

While general terms and conditions in the vendor contract would be based on the standard legal frameworks for procurement, vendor contracts would also include special conditions which could be key for the success of an ID system. The illustration above (figure 0.3) provides an overview of the various legal considerations that should be addressed in vendor contract(s).

By carefully designing a robust procurement strategy and systematically executing the procurement processes, ID authorities can lay the foundation for a strong and sustainable ID system.

1. ID SYSTEM LIFECYCLE

As a foundation for the development of the ID procurement checklist, extensive research has been undertaken which included:

- A study of procurement processes adopted for ID systems by various countries across the world
- Consultations with key global experts and practitioners in this domain

The four phases in the lifecycle of an ID system implementation, are illustrated in figure 1.1.

Enabling Tenets of an ID System

It is recommended that the conceptual design of a digital ID system is preceded by clear articulation of enabling tenets upon which the system will be based. These tenets include:

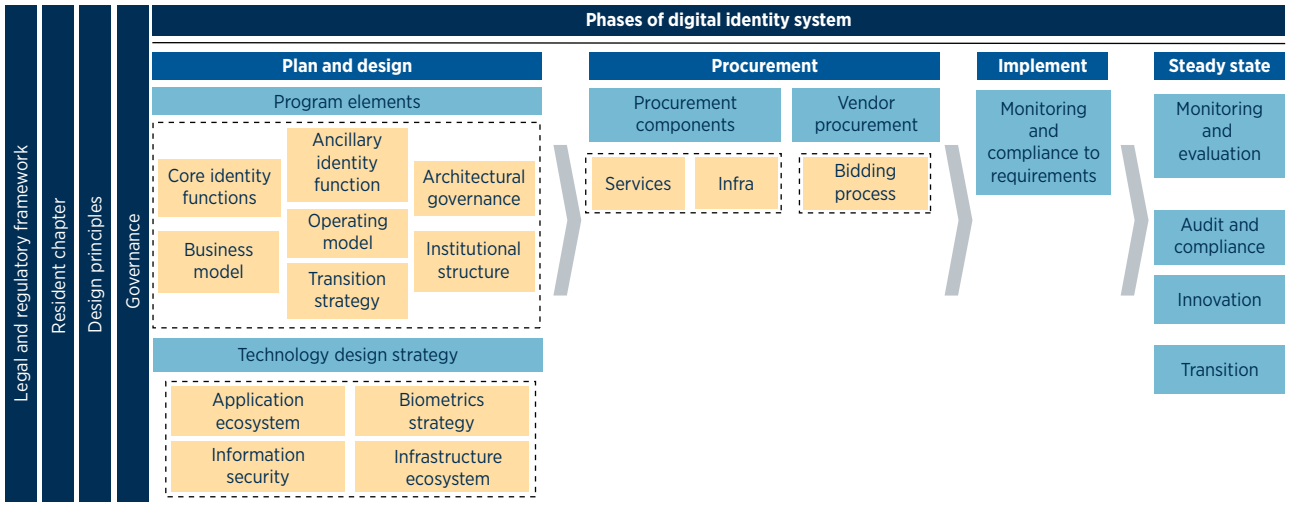
- A comprehensive legal framework that provides the appropriate policy and regulatory basis for the proposed ID system
- An actionable resident charter that delineates the service level offered by an ID system to its end users
- Critical programmatic and architectural principles that govern the ID system design
- A strong governance framework to ensure compliance to policies and standards

Legal Framework

Defining an appropriate legal framework is the first important step that governments should consider when building an ID system. It is an important program priority for any ID system because this helps to build trust in the system. This legal framework should therefore provide for a transparent and cohesive set of policies and regulatory guidelines that govern the collection, management, and use of an enrollee's personal data by all authorized participants in the ID system.

Such a legal framework enables a legally tenable ID credential that will be recognized by public and private sector service providers helping them to provide services based on authentication of their ID credential.

FIGURE 1.1 Lifecycle of a Digital Identity System



This section briefly explains the key design prerequisites and elements for an ID system implementation, followed by a detailed review of the "procurement phase" in subsequent sections.

[1] World Bank. 2018. *Principles on Identification for Sustainable Development: Toward the Digital Age*. Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age.

Although the legal and regulatory framework may vary from country to country, the laws that could enable the implementation and sustainability of an ID system are the following:

- ID law
- Civil registration law
- ICT laws
- Data protection law
- Citizenship law
- Cybersecurity law

A more detailed understanding of the legal framework associated with the implementation of ID systems and their implications for public services is provided in the G20 Digital Identity Onboarding report[2] and the ID Enabling Environment Assessment (IDEEA) Guidance Note.[3]

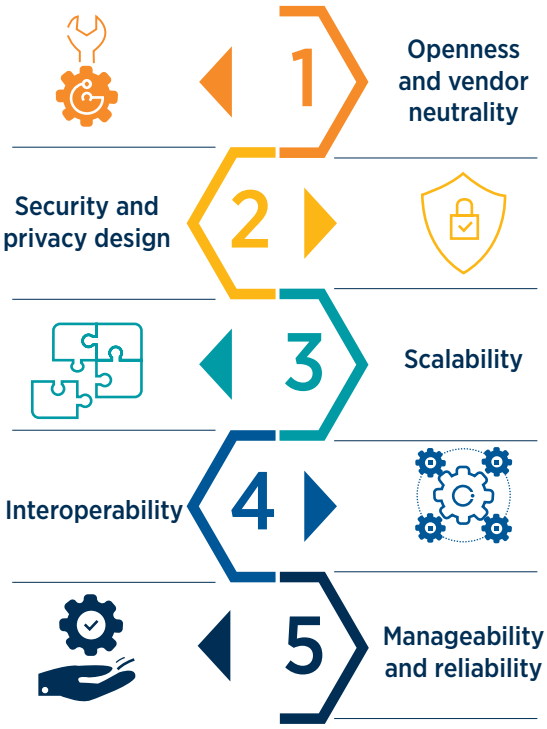
Resident's Charter

A "resident's charter" from the ID authority represents the commitment by the government towards providing seamless and accessible identity services to people in the country (similar to a minimum service performance agreement). Such a charter outlines directional guidelines for the ID authority to ensure quality and time-bound service delivery, provisions for grievance redress, and transparency and accountability in all processes dealing with resident data. A strong resident's charter is a key component in successful ID system implementations.

Architecture Principles of an ID System

Based on the requirements outlined in a country's legal framework and resident's charter, the ID authority may prescribe overarching design principles that will drive the implementation strategy of the ID system, for example, as in the shared principles developed by the ID4D initiative.[4] An overview of the architecture principles is presented in figure 1.2.

FIGURE 1.2 Architecture Principles



A. Openness and vendor neutrality

Avoiding vendor lock-in should be a key requirement for large ID system implementations. This can be achieved by following open standards and technology solutions that are less or not dependent on proprietary components. Openness in the ID system design is also enabled by vendor-neutral technology interfaces and open data formats. This is important for the following reasons:

- To ensure the long-term sustainability of the ID system.
- To provide ID authorities with the flexibility to adopt the best technology products available from different vendors.
- To ensure cost-effective services.

B. Security and Privacy by Design

Safeguarding personal data in an ID system to prevent unauthorized access and/or alterations of an individual's data must be a foundational principle. This includes adopting internationally accepted norms and best practices, as well as having the necessary legislation for privacy and data protection.

[2] GPFI. 2018. G20 Digital Identity Onboarding. Washington, DC: World Bank Group. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf.

[3] World Bank. 2018. ID Enabling Environment Assessment (IDEEA) Guidance Note. Identification for Development. Washington, DC: World Bank Group. http://documents.worldbank.org/curated/en/881991559312326936/ID-Enabling-Environment-Assessment-Guidance-Note.

[4] https://id4d.worldbank.org/principles.

The security strategy for an ID system should broadly comprise of:

- Defense in depth: The principle of "defense-in-depth" ensures layered security mechanisms that would increase security of the ID system. If an attack causes one security mechanism to fail, other mechanisms may still provide the necessary security to protect the system.
- Secure by default: All personally identifiable information (PII) should be encrypted both "at rest" as well as "in transit". PII data must be secured at all times, and there shall be no direct access to it other than through well-designed services.
- Run with least privileges: A system user should be provided with minimum rights and privileges, just enough to perform the intended function.
- All the hardware assets used in an ID system must be secured throughout their lifecycle as they may contain sensitive data even after being decommissioned.
- Different parts of a dataset might need different security classification.

Privacy pertaining to a resident's PII data is a cross-cutting principle across all design elements of an ID system. The privacy of an individual's data should be considered as a fundamental right. Hence, ensuring the compliance with the prevailing data protection and privacy laws of the country is critical to the success of an ID system. Privacy of residents is ensured by clearly defining what data is collected, the permissible uses of the data, and by ensuring that data is not shared with other entities without prior permission and consent of the user. The data privacy strategy should also accommodate the "right to be forgotten" function in the ID system design. Privacy of residents can be ensured through several approaches, such as:

- The ID system should follow a minimalistic approach around the collection of demographic and biometric data. It is advisable to only collect data that is required to ensure unique identity of residents and for issuing a unique identification number (UIN).
- The UIN issued as an ID number should be completely random and with no built-in intelligence to limit the profiling of residents.
- The data collected to issue a UIN must be only used for the identity verification and authentication of residents and this data must not be shared to external entities without appropriate legal authorization.
- For public reporting purposes, there should be provisions only for sharing or displaying aggregated data of an enrolled population
- Using advanced encryption and anonymization mechanisms, to ensure security of the data collected from individuals.
- Adopting features such as tokenization or pseudo anonymization.[5]

C. Scalability

During the course of an ID program, the amount of data managed by the ID system increases over time and hence adequate attention must be given to strengthen technology and processes on an ongoing basis. This can be achieved by the following measures:

- Ensuring the technology infrastructure is able to scale horizontally (for compute and storage requirements), that is, enable additional system resources to be added without having to shut down the core system components.
- Loose coupling of the components through APIs.

D. Interoperability

Globally, ID systems are increasingly being designed using a platform-based approach, where the service components are defined to be modular in nature. Embracing open interoperability principles is an essential requirement, to support seamless integration between the ID system and third-party systems (of both public and private agencies) for delivering public services to the end users.

E. Manageability and Reliability

ID systems undergo many changes over time, including legal, process, and technology-related changes. Hence, manageability (that is, ease of

[5] For more information, see World Bank. 2018. *Privacy by Design: Current Practices in Estonia, India, and Austria*. Washington, DC: World Bank. http://documents.worldbank.org/curated/en/546691543847931842/pdf/132633-PrivacyByDesign-02282019final.pdf.

implementing changes) of an ID system is important. At the same time, it is important for the system to handle failures resiliently and to require minimum human intervention. The ID system must be resilient against hardware and software failures and avoid any single point of failure. Continuous monitoring of service components within the ID system is necessary to ensure adequate integrity of data and uninterrupted availability of business processes.

Governance

ID authorities need to frame policies and administrative procedures pertaining to many key components and activities – such as the oversight of the different participating agencies involved, periodic review of the technology infrastructure, management of human resources, timely management of issues or grievances from service providers and residents, and budgeting and planning, among others – to ensure smooth running of the ID system. A strong governance model ensures that there is effective performance monitoring and control of service delivery and quality.

Phase I – Plan and Design

This phase plays an essential role in drafting of the procurement strategy by ID authorities. Before commencing on the ID system design, it is recommended that ID authorities carry out preliminary studies (for example, social surveys, underlying telecommunications environment studies, cybersecurity and privacy assessments, review of any legacy ID systems, among others) to gauge the current landscape. This will aid in estimating the necessary human resource efforts, costs and implementation timelines. The design should ensure adherence to the legal and regulatory framework and resident charter for the country. This phase forms the foundation for procurement of services and infrastructure by articulation of the program elements of the ID system, such as:

- Core identity functions, which includes enrollment, verification, authentication, and service ecosystem.
- Ancillary identity functions, which includes important supporting services and function such as customer relationship management, training, testing and certification, capacity building, and information, education and communication (IEC) strategy.
- Other key elements, such as architectural governance, institutional structure, business model, operating model, and transition strategy.

Based on these considerations, a technology design strategy may be developed at the end of this phase. For more information on the plan and design phase, see appendix A.

Phase II – Procurement

The plan and design phase defines the overall architecture of the ID system and drives the next key phase in the ID system lifecycle – the procurement phase. Transparent, open, and competitive bidding are fundamental to ensuring good and sustainable procurement practices. The procurement phase of an ID system encompasses two stages:

A. Development of Procurement Strategy

ID authorities need to outline the procurement strategy for procuring services and infrastructure to build, operate, and maintain an ID system. A procurement strategy development involves:

- In-house capability assessment
- Market analysis and vendor consultations
- Risk assessment
- Evaluating the procurement options
- Developing procurement considerations for IT components.

Table 1 highlights some global best practices to be considered while designing procurement strategies for ID systems.

Box 1.1 provides an example of lessons from the procurement process in the implementation of India's ID system.

TABLE 1.1 Best Procurement Practices

	Practice	Impact
1.	**Develop in-house technical expertise**	If in-house technical expertise is not available to the ID authorities for executing the procurement process, they could leverage international technical expertise for support in the technical design as well as the procurement phases. However, ID authorities should adequately plan to build their own capacity over a period, to avoid being unduly dependent on vendors and thus resulting in a vendor lock-in leading to a higher program cost.
2.	**Ownership of key technology components**	A procurement model should provide for government ownership over data and key technology components and should enable seamless transfer of system management and services to alternative providers. If the ownership does not rest with the government, it may result in risk of vendor and technology lock-in and data privacy issues.
3.	**'Architectural isolation' of niche technology solutions**	For certain cases where proprietary technologies are unavoidable (e.g., biometrics) innovative procurement strategies like multivendor arrangements and insistence on seamless plug and play interfaces could be evaluated and adopted in the ID system procurement processes.
4.	**Open competitive bidding**	Emphasizing an open and competitive procurement process that gives no special advantage to any specific set of vendors.
5.	**Adoption of performance-linked models**	Performance-linked contracts bring greater vendor accountability and enable efficient use of program resources. ID systems will be able to leverage improvement in the solution over time. Provision of performance-linked procurement models in such complex ID systems is an efficient way of managing vendors.
6.	**Well-defined terms of licensing model**	The licensing model for the tools/infrastructure/software, etc, should be clearly specified whether it is perpetual, device based, annual subscription based, etc, as it may have a huge cost impact and may lead to a lock-in of the critical information.
7.	**Encourage domestic participation**	Provisions for opportunities for participation of domestic vendors will ensure that in-country capabilities are developed resulting in less reliance on external vendors as well as paring down the additional cost.
8.	**Clear articulation of roles and responsibilities**	Articulating roles and responsibilities of human resources ensures smooth running of the system. It will also enable better program governance.
9.	**Avoidance of vendor and technology lock-in**	Conscious effort to avoid vendor and technology lock-in can prevent multiple risks because of dependence on vendors, such as increased costs in the future and data portability.
10.	**Specifying the right service level agreements**	This is vital to ensure satisfactory levels of service on a continuous basis.
11.	**Appropriateness of bill of materials (BOM)**	Bill of materials (BOM) should be accurate with clear specification of sizing and quantity. It will assist vendors to meet commercial requirements and can prevent discrepancies among bids.
12.	**Ensure interoperability and use of open standards**	Having a clear vision of the need for interoperability and open-standard driven technology will provide ID authorities with enough flexibility to easily upgrade critical system components with lower vendor dependency.
13.	**Consultation with the potential vendors**	Having consultative workshops with potential vendors provides governments with an opportunity to gauge the market interest for the ID program, as well as apprise themselves of modern and emerging trends in ID system technologies. It also increases competitiveness and reduces the risk of technology lock-in. Feedback from vendors in other countries can assist governments in achieving their stated objectives.

Box 1.1: Lessons from the Procurement Process of India's ID System, Aadhaar

India's ID authority, the Unique Identification Authority of India (UIDAI), implemented a partnership model with third party agencies to manage enrollment and data update operations. This approach helped in combining the infrastructural capacity of the government and the technical expertise of private agencies to build a system to ensure better service delivery to residents.

Adopting an outcome-based approach also helped in scaling the solution, as well as the ability of the underlying technology to seamlessly handle UIDAI's evolving requirements. UIDAI conducted several proof-of-concept exercises and field tests to determine the capability of various solutions available in the market and benchmark against their own requirements.

Adopting a unique biometric design strategy – with several automated biometric identification system (ABIS) vendors – also helped avoid vendor lock-in, and increased scalability of the system. This also ensured that the biometric vendors were constantly competing to improve their speed and accuracy. The use of three ABIS vendors (and thereby, three different proprietary algorithms) helped in establishing vendor and technology neutrality.

UIDAI also used a two-pronged technology design approach – open standards and open APIs – which helped them to promote competition among vendors, thereby enabling UIDAI to deploy the best-in-class solution for Aadhaar.

India's Aadhaar system relied on a competitive, standards-based (plug and play) procurement model. It emphasized standards that promoted transparency, accountability, scalability, and technical compliance. These, as well as real-time quality monitoring, allowed flexibility in the procurement process and drove competition among vendors, thereby limiting costs.

Source: https://www.nipfp.org.in/media/medialibrary/2016/09/WP_2016_176.pdf.

B. Procurement Process

This stage includes preparation of the request for proposals (RFP) and managing the bid process to select and onboard the vendor(s) for services and infrastructure needs and awarding contract(s) to the selected bidder(s).

Preparation of an RFP to procure suitable vendors is the vital stage in the procurement phase; where the ID authority shall take necessary precautions to avoid any pitfalls. An overview of many recommended provisions to be included in ID system RFPs is highlighted in figure 1.3. A more detailed view of the various components of the procurement process is provided in appendix A.

FIGURE 1.3 The "Dos" of the Procurement Process

Phase III – Implementation

After the procurement of services and infrastructure components, ID authorities need to implement the ID system. This phase will cover the execution of planned development activities, roll out the ID system, and integration with third-party service delivery systems for providing services, and so on.

During this phase, there should be continuous monitoring to ensure the comprehensiveness of the implementation activities (as against the requirements stated in the RFP(s)), as well as ensuring adherence to process and technical specifications, contractual conditions, and implementation timelines. For more information, see appendix B.

Phase IV – Steady State

After a successful deployment of the ID system, ID authorities needs to continuously monitor the performance of the system and the vendor, user experience and the changes taking place in the ecosystem to ensure sustainability of the program. This will drive refinements, upgrades, and innovations to ensure better performance and user experience.

This phase should also provide for:

A. Monitoring and Evaluation

It is critical to have a consistent and standardized management and monitoring process,

that serves as a strong control mechanism for ID authorities and service providers, during the delivery of ID-based services to residents. Once the services are planned, designed, and procured, they need to be supervised and monitored for:

- Ensuring zero disruption of services
- Meeting service levels
- Compliance to planned budgets
- Operational efficiency
- Fraud prevention
- Calibration and technological refreshes.

Monitoring and evaluation processes include a periodic review of enrollment processes, personnel and infrastructure to ensure quality, efficiency, and effectiveness. ID authorities will need to first define certain performance levels across various services and processes, which would then be measured against actual performance. This would help in independent evaluations of the ID services.

A good monitoring framework will also clearly outline the personnel who will carry out the evaluation, the frequency of evaluations, and the necessary actions to be undertaken in case the service levels/parameters are not met.

B. Compliance Audits

This will ensure a comprehensive review of the service providers' adherence to guidelines. The audit reports evaluate the strength and thoroughness of compliance to specified processes, security policies, user access controls, and risk management procedures.

This phase of the ID system lifecycle also includes the following to help wider adaption and continued sustainability beyond initial contract:

C. Enabling Innovation

ID systems can be the foundation for public and private agencies to build a viable services ecosystem for residents. The adoption of such an ID system ecosystem will benefit residents. ID authorities will have to generate reusable components and solutions which can be leveraged by public and private agencies. Multiple innovative strategies can be adopted by ID authorities, such as;

- Service catalogue – ID authorities should seek to continuously introduce new services, as well as simultaneously enhance services levels provided for existing services, through technological innovations.
- Channels – ID authorities should provide new channels for improving convenience to residents.
- Privacy and security – ID authorities should continuously strive to enhance security and privacy by implementing best practice.
- Technology innovation – Based on the analysis of user needs and services that deliver real benefits, this could be achieved by:
  - Enhancing performance of systems
  - Eliminating vendor specific components by developing in-house or leveraging open-source components to reduce cost of technology
  - Automation of routine activities
  - Using emerging technologies, such as artificial intelligence (AI) and machine learning (ML) to bring process efficiencies

D. Transition strategy

ID authorities have to make many important decisions around the procurement or renewal of services and infrastructure components once the contract expires. Therefore, they should have a detailed transition strategy to migrate the ID system components from one vendor to another.

Chapter 2 provides further detail on each of the phases and the factors that influence the system design and procurement choices for ID authorities. For more information, see appendix C.

2. A DETAILED VIEW OF THE PROCUREMENT PHASE

This chapter elaborates the various activities undertaken in the procurement process once the plan and design" phase is completed. ID authorities are expected to take key decisions with respect to procurement of services and infrastructure.

Procurement Strategy

Prior to selection the vendors for implementing the ID system, the ID authority needs to formulate an overall procurement strategy. This section details the key decisions and options for ID authorities in the procurement strategy, as well as the advantages and disadvantages of the different options.[1]

Assessment of In-House capability

The ID authority's in-house technical expertise, in terms of both constraints and enablers, will significantly affect the procurement strategy. Therefore, ID authorities need to undertake a detailed assessment of the following.

Capability in Managing the Procurement Process

The key considerations while assessing the capacity and capability of the ID authority in terms of procurement process are:

- Resources with experience and capability in bid process management including defining evaluation criteria, scope of work and legal terms and conditions and contract management.
- Technical capability to detail technical and functional specifications for products and services of the solution.

Capability for Development and Management of Various Solution Elements

ID authorities have to decide which of the services and infrastructure components are to be procured versus which can be developed in-house. ID authorities should evaluate their in-house capabilities and include or exclude specific services or infrastructure components for outsourcing and plan for in-house capacity development of critical elements.

Market Analysis and Vendor Consultation

A thorough market analysis exercise will allow ID authorities to understand the landscape of potential bidders, how they operate as well as the various products and services they offer. This would also give authorities an opportunity to seek input on the proposed scope of work and proposed solution for the ID system. This feedback can be used to make the necessary alterations in the scope of work and develop a more comprehensive RFP and make it more attractive to bidders. Through this exercise, an ID authority can assess a timeline for the IT infrastructure to be delivered and commissioned according to which key decisions could be taken.

The market analysis could be done to evaluate the following:

- Assess the number of potential bidders who can successfully execute the complex project and whether to allow foreign firms to participate in case of absence or scarcity of competent local vendors.
- Likely challenges in executing the project (for example, implementation timelines, supply-chain issues, payment issues, among others).
- Fair price of the solution.
- Feasibility of the proposed solution.

Risk Assessment

The aim of a risk assessment exercise in an ID program is to identify the risks involved in the execution of the project, both during the procurement and after onboarding the vendor. Table 2.1 elaborates the potential risks that could occur during the procurement cycle, as well as the impact on the procurement process with possible mitigations.

Box 2.1 provides an example of how poor articulation in the planning and design of an ID system can lead to challenges in the procurement phase.

[1] For more information on dos and don'ts in the procurement, please refer to the World Bank procurement guidelines.

TABLE 2.1 Risks and Mitigation During the Procurement Cycle

	Risk	Impact	Possible Mitigations
1.	Noncompetitive bidding process	- Genuine bidders do not participate - Procurement delays - Increased prices and poor value-for-money - Reduced quality of services - Reduced lifespan of assets	- Increased procurement oversight - Open competitive bidding based on market analysis and industry consultations - Complaint handling mechanism - Introduce or strengthen e-procurement systems - Ensure widest competition through global tendering
2.	Procurement process does not meet international standards	Procurement processes are inefficient, ineffective, not transparent, or unfair leading to increased prices, reduced quality, procurement delays and loss of funding allocation	- Comprehensive public procurement law - Open competitive bidding - Enable use of e-procurement system - Ensure widest competition by international advertising
3.	Poor procurement planning and inadequate information in terms of technical specifications, contracting strategy, etc.	- Increased prices - Purchase of unsuitable products or services - Procurement delays - Reduced lifespan of products - Reduced quality	- Strengthen project preparation activities - Hire specialized technical assistance for procurement - Appropriate quality specifications for the products - Appropriate service level specifications for services
4.	Deficient contract management	- Contract failures - Increased prices - Reduced quality - Inefficiency	- Contract management provisions are included in the RFP - Assign contract managers with defined duties and responsibilities - Good project management unit (PMU)
5.	Limited oversight of procurement and fraudulent practices	- Reduced competition - Increased prices - Reduced quality	- Effective governance mechanism with third-party review of procurement process - Measures to strengthen transparency - Better complaint handling mechanism
6.	Variation in scope or costing after contract award	- Quality of work delivered by the bidder decreases - Bidder does not focus on certain services or can deliver low-quality products in the latter phase of the project	- Improve specifications and cost estimates (hire external technical assistance in case of limited capacity) - Include as much background information as possible in the terms of reference, such as, but not limited to: overall strategy, business objectives, strategies, detailed current state assessment, appropriate architecture diagrams (even for out-of-scope systems that would need to be interfaced with) - Insert comprehensive statement of work (sharing of responsibilities between main parties for the implementation, operation and maintenance of the systems) - Strong contract management
7.	Abnormally low or high bids	- Contract prices increases (e.g. change requests, etc) - ID authority loses the flexibility to negotiate on certain conditions	- Strong prequalification criteria to carefully assess and weed out low-quality bidders who are trying to buy the contract - Design strong technical qualification criteria so that deserving bidders can score good marks - Final selection criteria should not solely depend on financial proposal but a mix of technical and financial proposal to ensure value for money
8.	Evaluation period takes too long	- Procurement timeline increases - Bidders loses interest - Technology evolves rapidly, and technical specifications can change significantly	- Evaluation should be made objective, to the extent possible - Inappropriate bidders to be removed during prequalification - Technical and commercial forms should be informative enough for easy scoring of the bidders

Box 2.1: Poor Planning and Design Leads to Challenges in Procurement Phase

A country in Africa tasked its national registration authority with the establishment and maintenance of a national identification register. The mandate was to create, manage, maintain and operationalize the register. Serious procurement problems delayed the project in 2010.

> In the country concerned, identity programs were run by different government agencies. Most identity systems were not interlinked. A commission was set up to create a national identity management system to enable secure, reliable and authentic verification of an individual's identity anywhere in the country and facilitated service delivery in government and the private sector.

The major challenges faced by this ID program include, but are not limited to, the following:

- Enrollment posed a central challenge for identity platforms to achieve nationwide coverage of data collection about citizens. Partnerships were one way by which the task of enrollment could have been managed. But, the country had limited success in partnerships to build its national ID system. For example, a US$236 million contract was awarded to a foreign company in 2001 to enroll the population and issue cards. The program ran for five years, registering 52.6 million out of planned 60 million people and issuing 37.3 million NIDs. However, the project was discontinued in 2006 because of allegations of impropriety over the contract award. Addressing the legacy of this failed project initially hampered the commission's implementation of a new ID card.
- Conducting biometric enrollment by each identity program lead to a substantial duplication of efforts, in terms of procuring similar devices and processes, issuing multiple identity credentials, maintaining multiple systems, and the residents having to provide the biometric and biographical information multiple times to several government agencies. An integrated identity program can offer significant cost savings and efficiency.

The country faced an urgent need to scale up national identity, integrating identity systems, cutting fiscal costs, and achieving efficiency in service delivery and management by addressing challenges more rapidly dealing with identity management. In light of these, the country's vision for identification requires refinement in terms of sharpening the vision of identification with an emphasis on rapid scale-up, full integration and cost optimization, strengthening the policy and legal environment, mobilizing the resources and scaling up with the speed.

Vendor or Technology Lock-in

Vendor lock-in is considered the biggest concern for the ID system implementation that should be addressed during the procurement process. Vendor or technology lock-in situations arise from using proprietary standards, vendor-specific software and/or hardware and complexity of ID systems with respect to technology, human resources, contractual terms. These cause increased cost and reduced flexibility to accommodate changes over time because the ID authority are locked-in to existing systems and are unable to take advantage of innovation or choose the most appropriate solution. The risk of vendor and technology lock-in can be mitigated by using open standards, interoperability in architecture, and strong procurement processes that avoids unnecessary conditions in the choice of technology and supplier.

Figure 2.1 presents a detailed list of pitfalls which can possibly cause vendor and technology lock-in and a mitigation approach to avoid the lock-in.

However, there are certain software solutions for which alternative, mature open source/standards-based technologies are not available (or are still evolving or have significant risks associated with them).

FIGURE 2.1 Issue and Mitigation for Vendor and Technology Lock-In

	Issues	Mitigation
Vendor Lock-in	Knowledge transfer	Systematic knowledge transfer
	Poor documentation	Timely documentation
	IP ownership	Ownership with government
	Data storage with vendor	Data residency
	Exit management	Standard transition and exit management
	Systems control	Admin rights with government
	Vendor staff dependency	In-house capacity building
	Source code control	Escrow account
Technology Lock-in	Proprietary software	Open software and open API solutions
	Proprietary data formats	Open storage standards
	Proprietary hardware	Commodity hardware
	Closed data exchange	Open exchange formats
	Proprietary standards	Open standards
	Non-standard devices	Multi-sourceable devices
	Non-standard encryption	Standard encryption ownership of keys

Impact of vendor and technology lock-in

- Higher costs
- Poor quality of service
- Frequent disputes
- Difficulty in change
- Poor commercial leverage
- Negative brand impact
- Limited innovation capacity

Benefits of vendor technology neutrality

- Cost competitiveness
- Good quality of service
- Easier change management
- Better innovations
- Flexibility to introduce new tech

In these scenarios, ID authorities are forced to use proprietary products. The ID authority should try to minimize the role of such products in their core architecture to the most extent possible or, at the least, these products could be deployed as distinct modules with integration via common APIs (preferably open in nature) reducing the effort required to replace one product with another. This approach allows the ID authority to replace them without much difficulty whenever possible and feasible.

Box 2.2 illustrates the case of procurement of an ID system in which vendor and technology is locked in.

Procurement Options

After conducting the market analysis, bidder consultations and internal assessments, ID authorities would then need to take several procurement decisions around various system components. The following steps should be followed by ID authorities during the procurement lifecycle of the ID system.

Step 1: Define and Design each Procurement Component

Procurement of Services

A. Application Development and Maintenance Services

These services include activities necessary to build, deploy, and maintain the ID system. It covers all software-related responsibilities of an integrated ID system implementation – including managing nationwide rollouts, overseeing all the third-party software development vendors, and ongoing implementation efforts to maintain and scale the system, across the duration of the contract. A high-level scope pertaining to this component would include:

- Architecting, designing, developing, and deploying the ID software applications.
- Ongoing maintenance and periodic upgrades for the ID software applications.

B. IT Infrastructure Services

The scope of services to manage and monitor the IT infrastructure include:

- Supply and deployment of IT infrastructure components that are necessary for the ID system. ID authorities may choose to either build their dedicated IT infrastructure, or manage upgrades to their legacy IT infrastructure, or engage third-party infrastructure service providers for software hosting purposes.
- Manage ongoing operations and upgrade of their IT infrastructure.
- Manage the annual maintenance contracts (AMCs) of infrastructure components procured from the market.

Box 2.2: Illustration of Procurement Resulting in Vendor and Technology Lock-In

In an upper-middle income country every citizen must be registered and issued an identity card within 30 days of turning 16 years of age or acquiring national citizenship. The National Identity Card is the prima facie proof of the citizen details stated on the ID card. It is a barcoded paper laminated identity.

They have a department that handles all the administrative functions, including card production, card distribution, enrollment, data storage and management, and card issuance and distribution. Only system maintenance and support are contracted out. The ID system is developed based on proprietary technology. The choice of a proprietary system has made it difficult to change vendors and prevents the department from developing in-house capacity to manage its identity infrastructure. Instead, it must rely on ongoing maintenance contracts with a foreign firm, at a price of US$3 million, which is over and above its yearly operational budget of US$5.6 million.

Another country similarly experienced vendor lock-in on the biometric templates stored on its smartcards. As a result, third parties were required to license this technology in order to read these templates, driving up the cost of developing an extensive point of sale (POS) network for authentication.

C. Biometric Services

If the ID authority is using biometrics, the scope of biometric services would include:

- Deduplication services.
- Authentication services.
- Fraud management services.
- Regular updates to deduplication and authentication algorithms.

D. Customer Relationship Management (CRM) Services

A CRM solution would function as the one-stop node for managing information requests/complaints and issues from key program stakeholders (residents and service providers). CRM services in ID systems should cover multilingual call-management technologies (such as Automatic Call Distribution (ACD), Interactive Voice Response System (IVRS), chatbots, and so on). ID authorities will need to scale-up CRM services as the program expands to more and more residents.

E. Information Security Services

The scope of work for such service providers could include services aimed at design and maintaining information security infrastructure, delivering information security services, active threat identification and mitigation, and managing periodic security awareness programs.

F. Testing and Certification Services

Testing and certification agencies for ensuring that the IT infrastructure procured is compliant with prescribed standards/guidelines, IT systems and data are secure, as well as to assess the capabilities of personnel deployed in the program.

G. Training Services

To ensure the smooth execution of the program, ID authorities need to ensure:

- Periodic assessments of the existing staff in the program.
- Designing and delivering appropriate training, aimed at improving the operational capabilities of the program staff. This entails developing a robust training program (encompassing key services, such as training content, information portals for self-learning, and classroom-based planned training sessions) for content dissemination.

H. Administrative Support Services

Managing day-to-day administrative needs (such as, facility management, human resource management, finance management, technical support services, among others).

I. Logistics Services

The scope for logistics-based services could include:

- ID credential distribution.
- Collection and transfer of beneficiary data records (for example, supporting documents) between the enrollment centers and regional/central offices.

J. Card Production and Personalization Services

The scope would be ID credential production and personalization needs of the program.

K. Information, Education and Communication (IEC) Services

The scope would include effective design and dissemination of information pertaining to the program to various users.

Procurement of Infrastructure Components

- Physical establishments (for example, administrative office facilities for the ID program headquarters, regional offices, enrollment centers).
- IT infrastructure components for the ID system. Based on whether the data center model adopted by a country is owned, collocated or cloud services; this procurement scope would change accordingly.
- Devices for enrollment (for example, biometric kits) and authentication (for example, POS machines).

Step 2: Decide on the Number of RFPs for Vendor Procurement

Once the procurement strategy and the scope of services are finalized, the ID authority should decide which services will be developed in-house and the number of RFPs to be issued (for example, one covering all services or multiple for individual services). This decision will be influenced by the current ability of the legacy infrastructure, if available, to meet the envisioned ID system goals. A higher number of RFPs to procure different services will result in an increase in the integration risks and effort, which the ID authority will need to manage. This could result in increases in cost and time-to-market. If purchasing a turnkey solution is not the chosen option, the integration risks could be minimized by use of international open standards and mature technologies – the skills for which, may be available with multiple vendors.

The different options have their advantages and disadvantages, as articulated in the sections below.

Single RFP Option

An ID authority can procure all services and infrastructure required for the program, under one single RFP. In this case, a single service provider may offer all the service components, or a lead bidder may bring in multiple service provider as a consortium and/or as subcontractors. This single vendor would own all responsibilities for delivering services outlined in its contract.

- **Advantages**
  - Lesser management oversight: This option is relatively easy to manage as it reduces administrative overhead as well as ensures that the accountability for meeting all contractual commitments (for example, service levels and timelines), rest with a single vendor.
  - Shorter procurement timelines: ID authorities need to evaluate only a single RFP and potentially save a lot of time for the contracting process and onboarding of the vendor.
  - Optimized effort and cost: The effort required to assess each bid component, for example, defining scope of work, pre-bid meetings, technical and financial evaluation, and obtaining multiple approvals, would be significantly less in case of a single RFP.
- **Disadvantages**
  - Inflexibility of the process: The ID authority may not be able to optimize multiple components as the whole solution is stitched together as a comprehensive offer by the system integrator (SI). Further, having a single RFP could also result in delay in the approval from government, especially as the total bid value could be high.
  - Limited number of participants: Including all services and infrastructure in one RFP increases the size and complexity of the contract. This may limit the number of potential bidders (who have the size and scale to execute such large and complex contracts) participating in the bidding process. This could exclude some smaller niche vendors who may have better capabilities and solutions for specific components (for example, application development and maintenance).
  - Higher dependency: In the case of a single RFP, the ID authority is dependent on a single vendor for all services. The ID authority may thus have limited flexibility to replace the vendor or introduce new vendors for specific components.

Multiple RFP Option

The ID authority may opt to procure the various services separately or from a few logical groups. In such cases, ID authorities need to decide on the services to be grouped together, balancing procurement efficiency, complexity in coordination, in-house expertise, preferred flexibility, and cost, as discussed above.

Step 3: Define the Procurement method

After finalizing the number of RFPs, an ID authority needs to determine the procurement method and bidding procedures (for each RFP, if necessary). There are various procurement methods that could be adopted by ID authorities; such as open competitive bidding, limited competitive bidding, direct contracting, and so on. The most preferred and globally followed procurement method is an open competitive bidding process, which gives the best value for money.

Step 4: Define the Bidding Procedures

The next step in the procurement lifecycle is to define the bidding procedures that would govern the technical and financial submissions from potential bidders. These procedures could either be a single- or two-stage process, as explained below. The bidding procedures can typically include either of the following:

- Single-stage process: The objective of a single-stage process is to prepare and issue an RFP directly to all the bidders and choose the right vendor (who fulfill all criteria and qualify) amongst them. It is recommended when the scope of work for the vendor(s) is well defined and ID authorities have limited time for the procurement process. It is also useful in scenarios where there are a limited number of bidders.
- Two-stage process: The two-stage process entails ID authorities shortlisting a set of potential bidders via an expression of interest (EOI) or a request for information (RFI) step, and limiting the RFP to this shortlisted group of bidders. In such a two-stage bid process, extensive details about the ID system's technical specifications are provided in the RFP. The two-stage process is relatively useful for large, complex programs with a varied scope of work (involving turnkey solutions, complex IT infrastructure components, and so on). For such large projects, it is recommended to conduct a prequalification round in the first stage to remove inappropriate bidders from the process. As the ID system contains critical and private data, it is advisable to limit disclosure of sensitive details pertaining to the ID system architecture to this shortlisted set of bidders alone. It is also common to have multiple bidder workshops to discuss clarifications around the scope of work or other contractual prerequisites with potential bidders. Such flexibilities are usually limited in single-stage bids.

A more detailed view of each stage in this 'two-stage' bid procedure is outlined below.

First Stage of a Two-Stage Process

The objective of this stage is to shortlist a potential set of bidders who have the requisite competency, capacity, and understanding of the solution required by the ID authorities. The following components could be considered in the EOI document:

- Invitation to the first stage of the contract.
- Introduction to the program.
- Broad scope of services.
- Prequalification (PQ)/eligibility criteria, including minimum and additional criteria.
- Bid submission forms and templates.
- Compliance sheet for prequalification.
- Request to bidders to suggest the solution.
- Bidder's experience in similar projects, spanning lessons, issues, and challenges faced, mitigation processes adopted, the eventual solution proposed, client expectations and feedback, among others.
- Bidder's specific credentials and accomplishments, for example, research studies published, patents and assets in ID systems.
- General terms and conditions.

This shortlisting process also helps in gauging the general interest levels of bidders for the project.

Second Stage of a Two-Stage Process

Only the shortlisted bidders from the EOI stage, will be qualified to participate in this second stage.

An RFP document can encompass the following components:

- Background information.
- Instructions to bidders.
- Prequalification (PQ)/eligibility criteria.
- Evaluation methodology.
- Scope of services to be performed.
- Deliverables.
- Implementation timelines.
- Payment schedule and conditions.
- Testing/quality assurance/acceptance testing mechanisms.
- Commercial bid template.
- Legal terms and contract conditions.
- Service level agreement.

- Annual maintenance contracts and warranty.
- Skills required.
- Resource deployment requirements.
- Exit criteria.
- Deliverable approval mechanism.
- Change order mechanism.
- Overall project governance mechanism.

A summary of key decisions to be taken in the two-stage procurement process is shown in table 2.2.

Procurement Considerations for IT components

The section below highlights the advantages and disadvantages of different procurement approaches, when dealing with IT components (both services and infrastructure).

Procurement of Commercial Off-the-Shelf Solutions (COTS) versus Open Source

The procurement of the commercial off-the-shelf (COTS) solutions is more suitable, when the open source technology alternative is not mature, or adequate technical support is not available for the ID authorities. ID systems are mission critical in nature and, hence, ensuring uninterrupted services is a critical expectation for authorities. Though open-source technologies offer solution autonomy for the authorities in the long term, having COTS products in the program can often give authorities a better service-continuity guarantee for critical IT components. An ID system design could include a fair composition of both open-source and COTS products in the solution. The considerations in evaluating COTS products in ID systems are:

- Level of technical support and shorter resolution timelines, as compared to the technical support provided by the open-source community.
- Time to delivery of solution.
- Upfront cost, costs of ownership, service cost, and consumables costs.
- Open API and open standard based deployment.

Procurement of Niche Services

Apart from COTS solutions, there are certain solutions that are more complex or proprietary in nature (for example, biometric solutions) that need to be procured as well. These solutions are particularly

TABLE 2.2 Key Decisions in the Two-Stage Procurement Process

Topic	Key decisions
Stage one of two-stage process	☐ Extent of the scope of the work to be shared ☐ Decide elements of capabilities for shortlisting ☐ Details on processes to submit the documents ☐ The timeframe for the participant actions in this stage, e.g., date of publication and submission, last date for queries submission, etc. ☐ Appropriate prequalification criteria and supporting documents that are necessary for evidence, such as: ○ Sales turnover ○ Net worth ○ Human resources strength of the organization ○ Project experience (number, value and specifications of the projects) ☐ Consortiums and/or subcontracting for the subservices of the contract ☐ Timelines for the EOI evaluation and shortlisting
Stage two of two-stage process	☐ The detailed scope of work and service level expectation ☐ Evaluation criteria and methodology ☐ Key milestones and timelines ☐ Provision for consultation workshop(s) with shortlisted bidders ☐ Timeline for the bidder actions

complex when considering specific implementation needs in the ID system design, for example, deployment, ongoing operations and maintenance, and integration with other ID system components. If not managed carefully, these solutions can prove to be a serious impediment for overall ID system service continuity. Some common challenges pertaining to the implementation of such niche solutions in the ID system, are:

- Duration of such contracts are relatively longer than usual, because of difficulties in adequate replacement of the solution. The cost of such replacements, when needed, can be a concern as well for ID authorities.
- As the technology market is evolving rapidly, there is a high likelihood that technical specifications of such solutions may be outdated, unavailable, or overpriced by the time the contract is awarded. This is especially true in the case of elongated procurement phases, thereby delaying the onboarding of the solution vendors on time.
- If technical specifications are poorly defined, the intended outcomes can deviate significantly from the real priorities of the ID program and potentially lead to vendor lock-in situations.

As an alternative to this dependency on niche vendors, ID authorities may try to develop their own open source-based bespoke solutions that gives them more flexibility. In such cases, it is useful to consider outcome-based procurement models to ensure the solution meets the necessary requirements, is periodically updated, and a plug-and-play deployment to ensure no technology and vendor lock-in.

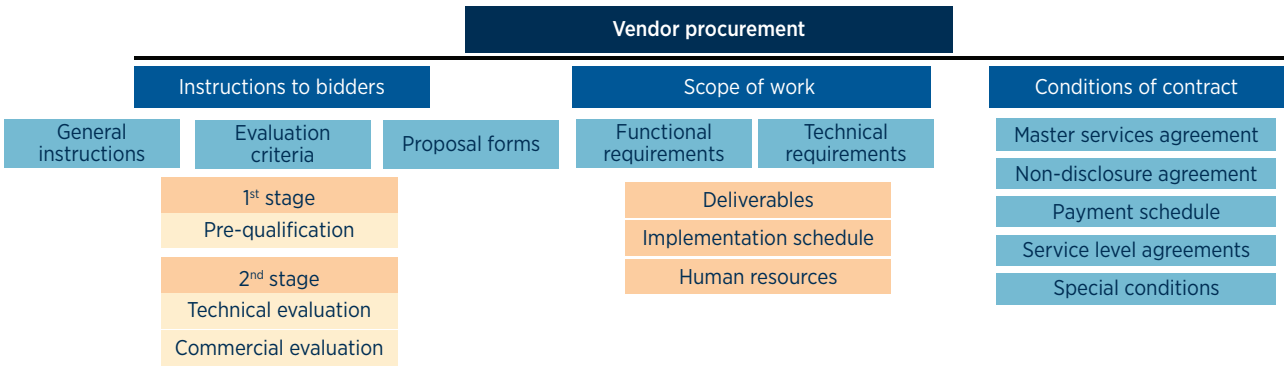
Procurement Process

ID authorities should define a robust bid management process to onboard the technically qualified bidder(s) at optimal cost. The procurement process must:

- Ensure that the ID authorities receive the scoped service components (that is, IT infrastructure, software solutions and products, non-IT services) at the best possible prices from the competing bidders.
- Ensure that there is no preferential bias towards any specific vendor and encourages competition.
- Draw upon the lessons of experience of the bidder(s) leading to a better outcome in the procurement lifecycle.

One of the most critical elements of the bidding process is preparation of a request for proposals (RFP) document that is based on the broader program strategy envisioned by the ID authorities. This document should clearly articulate the technical and financial evaluation criteria for the bid, a summary of the current infrastructure and services landscape, a detailed scope of services expected from suitable bidders, and overall contract conditions that would govern the contract between the government and the selected bidder(s). ID authorities must encourage a diverse set of stakeholders to contribute in the RFP document design (for example, industry experts, governmental advisors) in order to make it more inclusive and unambiguous for the bidders. If necessary, the ID authorities can set up specific technical committees to strengthen the procurement process design. Figure 2.2 provides an overview of key components of an RFP, in the vendor procurement process.

FIGURE 2.2 Key Components of a Request for Proposals



Instructions to Bidders

The RFP document must provide detailed instructions, on the following, to the bidders:

- Evaluation criteria
- Proposal forms

The checklist in table 2.3 provides guidance to ID authorities when designing this section of the RFP. The table encapsulates the common questions that need to be carefully considered and validated, to ensure that this RFP section is comprehensive and clear enough for bidders to respond without any concerns.

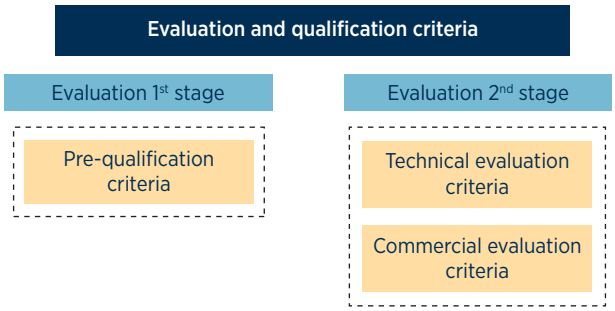
TABLE 2.3 Instructions to Bidders

Phase: Procurement Component: Vendor Procurement Area: RFP Instructions to Bidders			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Have the general instructions been clearly defined?		
2.	Has the project duration been clearly defined?		
3.	Are eligibility requirements clearly presented?		
4.	Have the conditions for disqualification of the bidder been clearly defined?		
a.	Is noncompliance to formats and procedures a disqualification criterion?		
b.	Will post-facto revision of bidder quote be considered as a criterion for disqualification?		
c.	Is deviation from terms and conditions of contract a disqualification criterion? Is there an option for bidders to propose deviation from the scope?		
d.	Is inability to provide necessary/required additional documents a disqualification criterion?		
e.	Is providing incorrect information a disqualification criterion?		
f.	Is attempting to influence evaluation through unfair practices a disqualification criterion?		
5.	Have the conditions for compliant and complete responses been clearly defined?		
6.	Is the right to terminate the process at any time, and not having any liability to provide any reason for the same, been clearly defined?		
7.	Have the steps for submission of proposals been defined (e.g., registration, preparation of bid, submission of bid, deadline to submit, etc.)?		
8.	Has the right to accept or reject any bid been defined?		
9.	Has the geographical coverage of the project been defined?		
10.	Is association with other bidders allowed (e.g., consortium or joint ventures)?		
11.	Is partnering with a local firm a requirement?		

Evaluation Criteria

ID authorities must clearly outline the evaluation methodology for the selection of the bidder(s). As explained in the section on bidding procedures, the evaluation methodology can entail a two-stage process, wherein prequalification criteria are applied to shortlist bidders in the first stage, followed by more detailed technical and financial evaluation criteria in the second stage (see figure 2.3). The first stage ensures bidder compliance against minimum organizational and technical parameters that are necessary to execute the process.

FIGURE 2.3 Evaluation and Qualification Criteria



Evaluation in First Stage

The evaluation criteria adopted in the first stage can be referred to as prequalification criteria. The objective behind using prequalification criteria is to encourage proposals from genuine contenders and solution providers. The criteria should be set to encourage competition and qualitative bid responses. The checklist in table 2.4 outlines key questions to be addressed by ID authorities when designing the 1st stage evaluation criteria.

Evaluation in Second Stage

Evaluation criteria adopted in the second stage encompasses the detailed technical and financial criteria of the RFP. ID authorities usually establishes an independent evaluation committee to perform the evaluation of technical and financial bids from all bidders. The checklist in table 2.5 outlines key questions to be addressed by ID authorities when designing the second-stage evaluation criteria.

Technical Evaluation Criteria

A clearly defined set of technical objectives and requirements ensures that the most competent

TABLE 2.4 Evaluation Criteria in the First Stage

Phase: Procurement Component: Vendor Procurement Area: RFP Evaluation Criteria (1st Stage)			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Are the evaluation criteria practical and flexible enough to encourage interested bidders?		
2.	Does evaluation criteria assess the high-level technical fit of the bidder against the stated scope or work expectations?		
3.	Does the evaluation criteria assess the financial capability of the bidder to execute the project?		
4.	Does the evaluation criteria assess the technical competence of the bidder, quality, and proven capability of the solution being adjudicated?		
5.	Does the evaluation criteria exclude bidders that been blacklisted by governments, multilateral institutions, or international companies (depending on procurement strategy)?		

TABLE 2.5 Evaluation Criteria in the Second Stage

Phase: Procurement Component: Vendor Procurement Area: RFP Evaluation Criteria			
#	Checklist item	Y/N/NA	Remarks
1.	Is an independent evaluation committee required for conducting the technical and financial evaluation of bids received?		
2.	Is the evaluation committee well versed regarding the objective and the process of evaluation?		
3.	Has the evaluation model been decided?		
a.	Is it a lowest price model?		
b.	Is it a quality and cost-based selection assessment model? Has the weight (percentage) between technical and cost proposals agreed upon?		
c.	Is it a quality-based selection process?		

TABLE 2.6 Technical Evaluation Criteria

Phase: Procurement Component: Vendor Procurement Area: RFP Technical Evaluation Criteria (TEC)			
#	Checklist item	Y/N/NA	Remarks
1.	Has the objective of TEC been clearly defined?		
2.	Does the TEC have a link to the scope of work?		
3.	Has the most relevant scoring/weighting scheme been used to evaluate bids?		
4.	Are the scoring guidelines clearly defined?		
5.	Are TEC defined objectively?		
6.	Does the scoring criteria exclude any bidder due to specific or restrictive criteria?		
7.	Does the bidder have to demonstrate the applications or proof of concept to showcase the functionalities and technical capability of the solution?		

bidder offering the right quality service(s)/solution(s) is selected for subsequent financial evaluation. Bid responses against these technical evaluation criteria is carried out by the ID authorities to arrive at a final (technical) score for each qualified bidder. ID authorities often specify a minimum score level to filter out bids that do not meet the requisite technical criteria. In most government procurements, only bidders who qualify against the technical evaluation criteria are selected for further evaluation against their financial bids. The checklist in table 2.6 outlines key questions to be addressed by ID authorities during this step.

TABLE 2.7 Commercial Evaluation

Phase: Procurement Component: Vendor Procurement Area: RFP Commercial Evaluation /			
#	Checklist item	Y/N/NA	Remarks
1.	Is there provision to examine the bids for arithmetical errors and rectification?		
2.	Will a bidder's failure to have the commercial bid signed by an authorized person, be treated as a nonconformance to the financial bid criteria?		
3.	Will any conditional bid (i.e., a bid which limits the bidder's responsibility to perform an activity) be treated as nonconformance to the financial bid criteria?		

Financial Evaluation Criteria

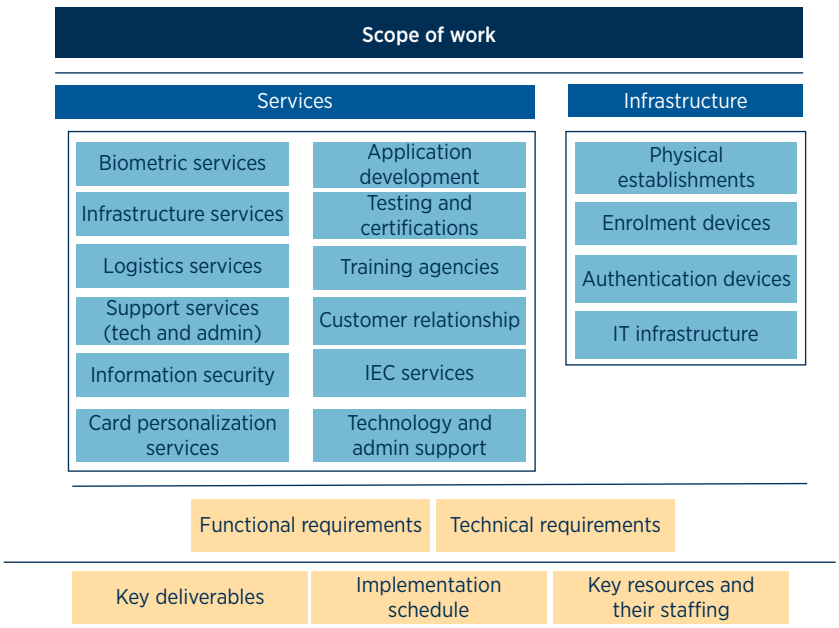
Once the technical scores are declared by the ID authorities, the financial (or commercial) bids of each selected bidder is evaluated. The checklist in table 2.7 outlines key questions to be addressed by ID authorities during this step.

Proposal Forms

It is advisable for ID authorities to outline specific formats and templates in which bidders are expected to submit their bid responses. Providing a specific proposal format makes it easier for the evaluators to compare bids and thereby complete the evaluation exercise satisfactorily. The following is a list of forms that may be provided through the RFP:

1. Covering letter
2. Bidder's general information
3. Power of attorney/board resolution
4. Declaration of subcontracted activities
5. Project summary
6. Resumes of key personnel
7. Summary sheet of financial proposal
8. Detailed financial proposal

FIGURE 2.4 Scope of Work



Scope of Work

The scope of work section of the RFP should include the following components, as illustrated in figure 2.4.

The RFP's scope of work that outlines the services and infrastructure components of the ID system, will be derived from the program strategy defined in the plan and design phase. Options for the design choices should be finalized after evaluating the advantages and disadvantages with the stakeholder group. Once finalized, these design choices will be translated into the functional and technical requirements that will be included in the scope of work. Defining a proper and structured scope of work is essential for the bidder(s) to clearly understand the requirements to

be performed under the contract. The scope of work can be further broken down into the following:

- Key deliverables and milestones
- Implementation schedule
- Key resources and staffing requirements

The checklist in table 2.8 outlines key questions to be addressed by ID authorities, while designing this section of the RFP.

TABLE 2.8 Scope of Work

Phase: Procurement Component: Vendor Procurement Area: Scope of Work			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Has the scope of work (encapsulating all requisite functional and technical requirements) been clearly defined?		
2.	Have the key deliverables and milestones been defined?		
3.	Has the implementation schedule been defined?		
4.	Have the key resources and staffing requirements been defined?		

Conditions of Contract

The RFP's conditions of contract section set down several contractual conditions under which the selected bidder(s) will execute the services. The major components of this section are illustrated in figure 2.5.

FIGURE 2.5 Conditions of Contract

Master Services Agreement

A master services agreement (MSA) is a contractual document that specifies the performance objectives and outlines the responsibilities of the parties involved (that is, ID authorities as the purchaser and the selected vendor(s) as the service providers). This agreement dictates the terms of agreement between the ID authority and the selected bidder(s). It clearly articulates generic terms in the contract, such as payment terms, product warranties, intellectual property ownership, and dispute resolution, among others. The goal of an MSA is to make the contractual process faster and transparent for both parties involved, as well as to facilitate and simplify contract negotiation.

Table 2.9 outlines key questions to be addressed by ID authorities in this section of the RFP.

TABLE 2.9 Master Services Agreement

Phase: Procurement Component: Vendor Procurement Area: Conditions of Contract Master Services Agreement			
#	Checklist item	Y/N/NA	Remarks
1.	Have the definitions and the interpretations for the MSA been clearly specified?		
a.	Has the mechanism to resolve ambiguities (if any) within the agreements been set down clearly?		
2.	Has the scope of the project been well defined?		
3.	Have the terms and duration of the project been defined?		
4.a	Have the obligations of the ID implementing authority been defined in the MSA?		
4.b	Have the obligations of the bidder been defined in the MSA?		
5.	Are conditions pertaining to financial matters been specified in the MSA, e.g., payment terms, invoicing, tax, etc?		
6.	Is there any form of performance guarantee mechanism to be used in case of default on part of the bidder?		
7.	Has the governing law(s) been defined?		
8.	Have the clauses for dispute resolution been specified?		
a.	Has a workable business solution been ensured, before resorting to formal procedures, such as steps 1-4?		
b.	Is the internal escalation process defined?		
c.	Is the mediation process defined?		
d.	Is the adjudication/expert determination process defined?		
e.	Is the arbitration process defined?		
f.	Have the time limits for resolution been defined?		
9.	Have the reasons and consequences of an event of default been defined (i.e., when there is any kind of failure to comply by the bidder)?		
10.	Have the clauses for termination of contract and its effect been defined?		
11.	Have the high level acceptance criteria been defined for various deliverables?		
12.	Have assignment/novation clauses been included to address situations where the service provider(s) undergo mergers or acquisitions or in case of their bankruptcy?		

Non-Disclosure Agreement

A non-disclosure agreement (NDA) is a legal contract between the ID authority and the selected bidder(s) that specifies confidentiality of materials and services in the contract, knowledge or information that either party wishes to share/disclose/restrict with one another, as part of doing business with each other. NDAs are entered upon between parties to protect the rights for their proprietary information and sensitive business-related information.

The checklist in table 2.10 outlines key questions to be addressed by ID authorities, while designing this RFP section.

TABLE 2.10 Non-Disclosure Agreement

Phase: Procurement Component: Vendor Procurement Area: Conditions of Contract Non-Disclosure Agreement			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Has the sensitive information of the program, been classified as confidential?		
2.	Has all the nonconfidential information of the program been defined?		
3.	Have the cases for access and restriction of confidential information been specified?		
4.	Is there a provision of security and prevention of unauthorized access of confidential information?		
5.	Has breach notification been defined in case confidential information of the program is advertently or inadvertently disclosed by the bidder(s),		
a.	Are the measures to notify the data owner defined?		
b.	Are the measures to rectify the issue defined?		
6.	Has there been consideration for a case wherein the bidder might be under a legal compulsion to disclose any confidential information?		
a.	For such a case, is there a timeline within which the bidder shall inform the ID implementing authority of the same?		

Payment Schedule

The payment schedule clearly defines the mechanism of paying the bidder(s) for the successful delivery of services and products during the project. It includes the schedule and specific terms governing payments to the bidder(s), for all the activities performed as part of the contract between the ID authority and the bidder(s).

The checklist in table 2.11 outlines key questions to be addressed by ID authorities when designing this section of the RFP.

TABLE 2.11 Payment Schedule

Phase: Procurement Component: Vendor Procurement Area: Conditions of Contract Payment Schedule			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Have the payment terms been clearly defined?		
a.	Is the payment schedule aligned with deployment and go-live of software system and not based on activation of individual product licenses?		
b.	Is the payment schedule post go-live aligned with provisioning of warranty support and annual maintenance activities?		
c.	Is a significant portion of project payments to the vendors provided for post go-live phase?		
2.	Is there a linkage between the payment milestones and a deliverable or unambiguous payment schedule (e.g., go-live)?		
3.	Has it been ensured that the payment value reflects the actual efforts of the contractor?		
4.	Are the payments linked to only one type of delivery – service/input or solution/outcome?		
5.	Have the payment dates and timelines been defined?		
6.	Has it been ensured that there are no penalties on payments that are not specified in the contract?		
7.	Has it been ensured that changes in government taxes are not imposed on the contractor by making payment adjustments?		
8.	Have the payment methodology and related calculations been well defined?		
9.	Have the key activities/milestones for payments been defined?		
10.	In case of a delay in payments, is the process defined? Is there adequate protection for service provider(s) in case payments are unduly withheld by the purchaser?		
11.	Is the process of raising invoices clearly defined in the RFP?		

Service Level Agreements

Service Level Agreements (SLAs) govern the quality and timeliness of service delivery during the implementation and operations and maintenance phases of an ID system. SLAs outline specific service level commitments (such as expected levels of service to be provided) expected of the bidder. It provides clarity in terms of service ownership, roles and responsibilities, and accountability.

The checklist in table 2.12 outlines key questions to be addressed by ID authorities when designing this section of the RFP.

TABLE 2.12 Service Level Agreements

Phase: Procurement Component: Vendor Procurement Area: Conditions of Contract Service Level Agreements			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Have the service level classifications been defined?		
a.	Have the target service levels (which are goals) been defined?		
b.	Have the minimum service levels (which are expected to be achieved) been defined?		
c.	Have the increased impact service levels (which are inferior levels impacting the business) been defined?		
d.	Has the SLA measurement protocol been specified?		
2.	Has the effectiveness of the SLAs been defined?		
3.	Have the consequences of failure of SLAs been specified?		
4.	Are the SLAs for the following indicative list of activities been ensured?		
a.	Project delivery milestones		
b.	System performance		
c.	System response time		
d.	Performance and availability of human resources		
e.	Recovery time objective (RTO) and recovery point objective (RPO) for disaster recovery and business continuity planning		
5.	Have the calculations and sample illustrations of the contract SLAs been clearly defined?		

Special Conditions

Apart from the above, there are some other special conditions that must also be considered while drafting the conditions of contract.

The checklist in table 2.13 outlines key questions to be addressed by ID authorities when designing this section of the RFP.

TABLE 2.13 Special Conditions

Phase: Procurement Component: Vendor Procurement Area: Conditions of Contract Special Conditions			
#	**Checklist item**	**Y/N/NA**	**Remarks**
1.	Have the intellectual property rights (IPR) for existing and new assets been defined?		
a.	Has it been decided who will own the IPR?		
b.	Is there a provision to license items such as products, solution source codes, and materials according to the terms of the license agreement?		
c.	Are the procedures for handing over the source code clearly defined, along with the appropriate technical documentation?		
2.	Has insurance cover been defined?		
a.	Does the bidder own the insurance cover?		
b.	Does the bidder maintain the insurance for public liabilities, product liabilities, and other types of insurance?		
3.	Does the source code belong in an escrow account to maintain the software?		
4.	Does the purchaser have ownership of annual maintenance contracts (AMCs), warranties and maintenance of the products and solutions?		
5.	Has the limitation of liability been defined?		
6.	Has the cap on liquated damages been defined?		
7.	Is data ownership defined?		
8.	Is data residency defined?		
9.	Is purchaser obligation defined?		
10.	Are bidders' obligations defined?		
11.	In case additional services or infrastructure are required during the duration of the contract, does the change order (change request) clause mention the clauses of when it can be invoked and by whom?		
12.	As the IT infrastructure to be procured for the ID system is already a part of the national critical infrastructure, are security clearances well defined in the document?		
13.	Are knowledge transfer terms and conditions well defined in the document?		

APPENDIX A
PLAN AND DESIGN

Implementing an ID system for a country requires a comprehensive planning phase that aligns the Government's envisioned strategic goals with a practical implementation strategy for rolling out in the country. It is imperative that this planning effort is taken up in all sincerity prior to procurement, so that all potential implementation risks are adequately addressed in the design and rollout of the ID system. Government priorities for the planning phase of an ID system include:

1. Outlining the key design principles to be considered and addressed
2. Defining and designing the various components of the ID system, like enrollment & data update, authentication, ID-linked service ecosystem and customer relationship management.
3. Defining the operating and business model, based on the objectives as set out by the Government. Specific considerations would include;
    a. Operating model – It refers to how the operations in the ID system are structured for different services. For example, which of the services will be developed in-house, which will be outsourced, and which will be executed in a partnership model.
    b. Business model - Government may have to adopt appropriate models of program financing to manage the budgets of the ID program). They may also opt to design effective revenue strategies (e.g. service fees for core ID services, as well as delivery of ID linked public services to citizens) to ensure long-term sustainability of the ID program. Government will have to choose an institutional arrangement that would be suitable and adaptable to the needs of the country. Some popular business models as evidenced in many ID systems around the globe include;
        i. Self- financed models like 'government funded'
        ii. Financed through a 'PPP' model such as BOT, BOOT, BOO etc.
        iii. International funding support like UNDP funded ID system in Malawi, World Bank in Morocco
        iv. Self-sustaining financing models (charging the services provided)
4. Defining the appropriate technology strategy of the program based on the objectives set out by a Government. Factors such as the existing digital landscape of the country, availability of the technical expertise of the human resources, modern industry technology trends, scalability needs of the ID program as well as learnings from many similar global ID systems, could also be important considerations in the eventual procurement of the ID system technology components.

The "Plan & Design" phase can be further segregated into two major considerations that ultimately impact decisions made by a Government during an ID system procurement lifecycle. These include:

A. Program Elements
B. Technology Strategy

FIGURE A.1 Key Considerations in the "Plan & Design" Phase of an ID System

Program Elements

The various design choices and decisions adopted in the ID system will go a long way in determining the success of the program. The ID authority should consult relevant stakeholders, to clearly prioritize the program goals and the direction for the ID system going forward.

An overview of the critical program considerations for an ID system is illustrated below:

These program elements are broadly categorized into the following:

- **A.** Core Identity functions
  - **a.** Enrollment and Update services
  - **b.** Authentication services
  - **c.** ID-linked services ecosystem
- **B.** Ancillary Identity functions
  - **a.** Customer Relationship Management services
  - **b.** Training, testing and certification
  - **c.** IEC campaigns
- **C.** Architectural governance
- **D.** Institutional structure
- **E.** Operating Model
- **F.** Business model
- **G.** Transition Strategy

A more detailed view of each of the above considerations is articulated in the subsequent section below.

FIGURE A.2 Program Elements

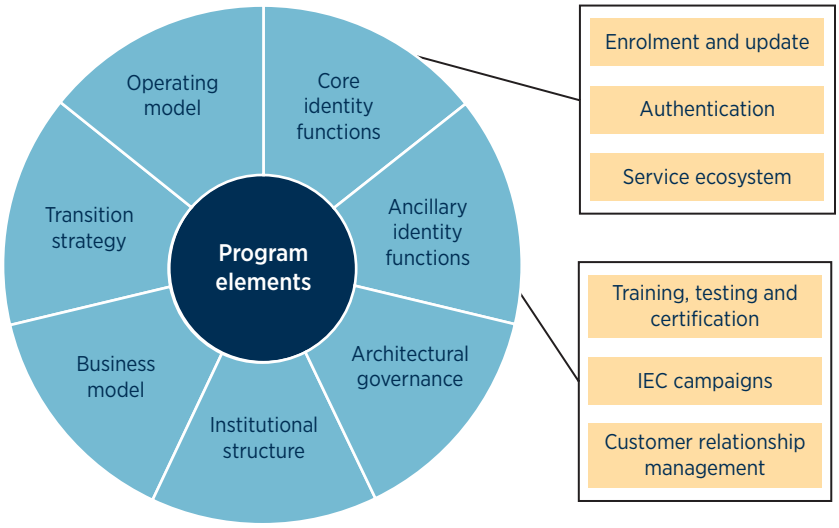
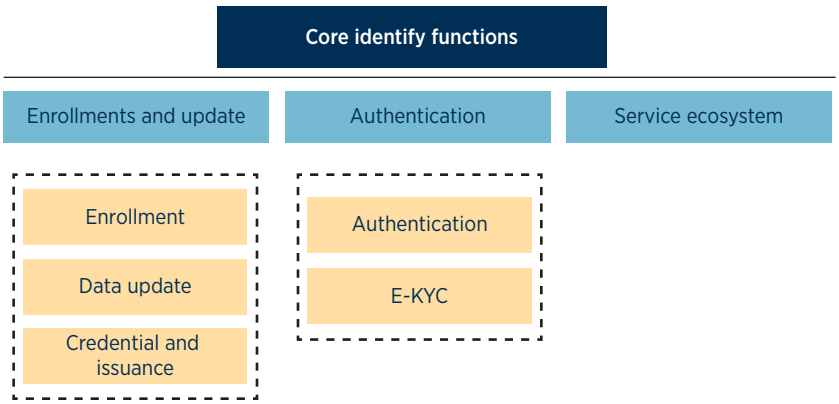


FIGURE A.3 Core Identity Functions



Core Identity Functions

The lifecycle of an ID system begins with the enrollment of eligible citizens and legal residents into the system, followed by the ongoing use of ID-based authentication services by viable partners at point-of-service, and provision of various ID-based services aimed at streamlining public and private service delivery for Citizens/Residents.

As illustrated above, the 'core identity functions' can be categorized into four distinct ID lifecycle sub-systems. The subsequent sections elaborate each subsystem in further detail.

Enrollment and Update Subsystem

Enrollment Subsystem

Processes and systems adopted by a Government in the "enrollment" phase of an ID lifecycle have implications on the successful coverage of all eligible residents, as well as to ascertain the quality and accuracy of the data collected during the enrollment process. ID authorities have to often make key decisions around various design choices in the 'enrollment' process – spanning technology, infrastructure and human resource requirements.

The enrollment sub-system should be designed in a way that ensures the following:

- Strong focus towards universal coverage of the eligible population.
- Processes are adequately designed to ensure the capture of high quality and accurate data.
- All components to be procured to be clearly articulated in the design itself.

The procurement decisions in an ID enrollment sub-system are influenced by various design elements and infrastructural components and services, as illustrated below:

Topic	Key Decisions
General	☐ Age criteria ☐ Inclusion criteria ☐ List of valid PoI/ PoR/ PoA documents ☐ UIN numbering scheme ☐ Validity of Identity ☐ Standard Operating Procedures for the enrollment process
Stakeholders	☐ Identifying the program stakeholders ☐ Defining the roles and responsibilities of the stakeholders
Enrollment Strategy	☐ Number of centers ☐ Number of Permanent and Temporary enrollment centers ☐ Modes of enrollment- Offline/ Online ☐ Percentage coverage year-on-year ☐ Finalizing the enrollment kit constituents ☐ Certifications of the enrollment kit for quality ☐ Enrollment strategy for exception scenarios ☐ Registration mechanisms for start-up and steady-state phases (e.g., by government staff, outsourced etc.) ☐ Strategies to ensure last-mile coverage
Data	☐ Core Identification data o Number of data attributes (Data minimization) o Mandatory and Optional fields ☐ Validation Data ☐ Metadata ☐ Data Quality guidelines ☐ Data storage guidelines ☐ Data Protection guidelines ☐ Data transfer to ID authority
Verification	☐ Data quality checks ☐ ID proofing rules and regulations ☐ Identity deduplication process design (including manual adjudication)

Data Update sub-system

This section includes the data update guidelines necessary for ID system. One of the important aims of providing the eligible population a digital identity is that the population can leverage it for better access of both public and private services. ID authorities must ensure that the information stored in the ID system is accurate, relevant and

up-to-date. The authorities need to provide a mechanism to all enrolled citizens and legal residents to update their data, on an ongoing basis. There are various design choices which will highlight the need to procure the necessary infrastructure and services.

Topic	Key Decisions
Data Update strategy	☐ Modes of Data update (Offline/ Online) ☐ Channels of Data update (self/ assisted) ☐ Types of services ☐ Minimum LOA for accessing data update services ☐ Data fields which can be updated ☐ Mandatory and Optional updates ☐ Business model for data update requests ☐ Location and number of service delivery centers ☐ Validation of documents for service delivery
Stakeholders	☐ Identifying the stakeholders like ID Authority, Enrollment agency, operators, residents etc. ☐ Defining the roles and responsibilities of the stakeholders

Credential and Issuance Ecosystem

This section of the procurement checklist highlights the ID credential and issuance ecosystem of an ID system. Citizens and legal residents that are being enrolled into an ID system, need to have a government approved identity proof document to prove their individual identities and avail various public and private sector services, etc. ID authorities need to carefully evaluate and consider various design elements that would result in the procurement of necessary infrastructural components and services like cards, printing devices etc.

Procurement decisions in a "credential and issuance" sub-system is influenced by various design elements and infrastructural components, as illustrated below:

Topic	Key Decisions

Credential and Issuance strategy	☐ Credential medium (Physical/ Digital)
	☐ Credential Issuance (yes/no) by the ID authority
	☐ Mode of issuance (offline/ online)
	☐ Age groups to which credential will be issued
	☐ Validity of the credential
	☐ Procedure for revocation and reissuance of credential
	☐ Logistics arrangement for issuance
	☐ Business model for credential
	☐ Credential design strategy
	  ○ Credential material
	  ○ Credential security
	  ○ Credential storage
	☐ Data points on credential (Human readable and machine readable) including disclosure of personal identifier(s)
	☐ ID authority to decide whether offline data of authentication will be stored on the credential

Stakeholders	☐ Identifying the stakeholders like ID Authority, Logistics partner etc. ☐ Defining the roles and responsibilities of the stakeholders

Authentication Subsystem

The authentication processes designed in an ID system ensure that an individual is the same person that they claim to be. This involves confirming the individual's identity by matching credentials provided by him/her, against one or more authentication factors (e.g., a PIN, password, or fingerprint). The combination of authentication factors should include some or all the following:

- Possession based – something that an individual demonstrates that they have, such as a physical or virtual card or certificate
- Knowledge based – something that an individual demonstrates the knowledge of, such as an identifying information like a PIN
- Inherent – something that some individual claims that they have, like an iris or a fingerprint scan

Procurement decisions in an "authentication" subsystem is influenced by various design elements and infrastructural components, as illustrated below:

Topic	Key Decisions
Authentication	☐ Authentication modes (Offline/ Online) ☐ Authentication ecosystem architecture (trusted, federated model) ☐ Authentication types (OTP based, Demographic authentication, Biometric authentication, etc.) ☐ Authentication services (Yes/no, e-KYC) ☐ Data points to display after successful authentication in different types of services ☐ Data guidelines for capturing, verification and storage etc. ☐ Scope and retention of authentication logs
Stakeholders	☐ Identifying the stakeholders like ID Authority, authentication partners etc. ☐ Defining the roles and responsibilities of the stakeholders

Service Ecosystem

The services ecosystem enables the residents to avail various services using the unique identification. It has a wide range of services with diverse roles, responsibilities and interests. These services can be in the form of government benefit services, financial and social inclusion, etc.

The roles and responsibilities of different entities like government, residents, private firms, etc, are clear and non-conflicting. Independent and neutral agencies are empowered to monitor and supervise the processes. There can be various establishments set up that provide these services to the residents. Processes such as e-KYC or biometric authentication ensure that the financial assistance reaches to those who need it.

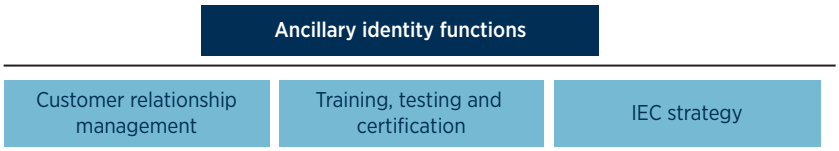
Topic	Key Decisions
Service ecosystem	☐ Services that the ID authority will offer to Service Providers (including SLA) ☐ Minimum LOA expected by the SPs for the end users to avail their services
Stakeholders	☐ Roles, responsibilities and allocation of liabilities between the ID authority and all ecosystem partners (trust framework)

Ancillary Functions of Identity Systems

In addition to the core identity functions in an ID lifecycle, ID authorities do often also have to make further procurement decisions to support these core functions, as illustrated below:

These could include decisions pertaining to end-user trainings, testing and certification of devices and systems, and an IEC strategy to ensure the smooth functioning of the ID program. More details about each of these functions are provided in the subsequent sections.

FIGURE A.4 Ancillary Identity Functions



Customer Relationship Management

A clear and streamlined administrative procedure is required to address grievances, and remedy identity theft or fraud. The enablement of user-friendly mechanisms for individuals to view their data, see who has accessed their data, edit or update information, and contact data centers to address any grievances is necessary.

ID authorities often look to establish a multi-partner ecosystem involving internal agencies, citizens/residents, and service provider(s), among others; during the implementation of the ID system. As an important program goal, ID authorities would need a system to support the citizens/residents around information, queries, issues, resolutions and grievances pertaining to the ID system. This could entail opening multiple user-engagement channels like email, messaging, physical centers, social media etc. with multi-lingual support.

Topic	Key Decisions
Customer Relationship Management	☐ Methods for handling queries (Voice, email, web portal, social media, chatbots, letters, walk-ins, self-help etc.) ☐ Number of languages in which the query handling services would be provided to be provided to residents ☐ Sizing requirements for the queries like no. of residents, enrollment/ day/ authentications/ day, working hours for the agents, no of agents, peak call volume, etc. ☐ List of services for which assistance would be provided ☐ ID authority to deploy grievance handling technologies including but not limited to Automatic Call Distributor (ACD), Interactive Voice Response System (IVRS) etc.
Stakeholders	☐ Identifying the stakeholders like ID Authority, contact centers, user agencies, internal divisions etc. ☐ Defining the roles and responsibilities of the stakeholders ☐ Plan for providing training to the agents and CRM staff

Training, Testing and certification

In any ID system, it is imperative that the Government and ID authorities consider comprehensive end-user trainings for the users of the systems (like enrollment operators, authentication agencies, call center agents) as a critical program priority. This is especially true when countries embark upon the deployment of nationwide ID systems in aggressive enrollment targets, which often results in a rapid scale-up of infrastructural components (e.g. enrollment centers, enrollment staff) in short timelines. This in turn puts a greater emphasis on training a greater staff count to meet the program targets within these short timelines. Alternatively, in the case of ID programs with longer enrollment timelines, the sustenance of staff capacity and capabilities is a key program requirement as well. In such cases, ID authorities may need to continuously hire and train new staff who lack the adequate skills (i.e. technology and process-based skills in an ID lifecycle), and to accept the chore of constantly retraining the existing staff as well. This is more likely to happen when temporary staff are hired to manage critical ID functions in the program. Overall program costs pertaining to these training requirements is another key factor that ID authorities are faced with, when designing ID systems.

Procurement decisions for these functions are influenced by the following design elements and infrastructural components, as illustrated below:

Topic	Key Decisions
Training agency	☐ Training mode (Offline/ Online) ☐ Phases of training ☐ Layers of training to various stakeholders ☐ Delivery of training ☐ Number of batches and batch size ☐ Training duration ☐ Training deliverables to trainees ☐ Refresher training ☐ Availability of training content (anytime, anywhere) to the authorized users
Content development agency	☐ Content development for training exercises regarding enrollment, authentication etc. ☐ Developing content for IEC campaigns etc.
Testing and Certification agency	☐ Spécifications for enrollment devices, authentication devices etc. ☐ Certification to enrollment operators etc.
Stakeholders	☐ Identifying the stakeholders like ID Authority, residents, different ministries etc. ☐ Defining the roles and responsibilities of the stakeholders

IEC Strategy

ID systems need to have a sustained focus towards public awareness and mass communication strategies aimed at diverse users and influencers for adoption. This is a critical program priority that determines the success of the ID system. For instance, these campaigns can be designed to address common questions from enrolees such as - Why is an ID important for them? What benefits can they avail from the government using this ID? What are the Government provisioned processes and channels through which they can manage updates to their unique identity record, among others. The likelihood of unenthusiastic residents necessitates the need for proactive public education and information campaign, aimed at encouraging their participation in the country's ID system. Campaigns for awareness and education, advertisements and commercials about the enrollment process is an important tool for cognizance. The cost for such awareness campaigns is typically at its peak during the enrollment phase of an ID system, and gradually keeps decreasing as the program enrollment targets are being met.

Typical procurement decisions in an ID system's IEC strategy are influenced by the following elements, as illustrated below in the table:

Topic	Key Decisions
Information, Education and campaign	☐ Resident engagement plan conveying the mandates and benefit of the ID program and creating a demand for the ID system ☐ Channels like social media, television, print media, radio etc. ☐ Coverage criteria like regional level, state level etc. ☐ Phases for IEC such as enrollment phase, service delivery phase etc. ☐ Target audience for the IEC phases ☐ Business model for the IEC program ☐ Content development for the campaigns including improvement through effective feedback mechanism
Stakeholders	☐ Identifying the stakeholders like ID Authority, IEC partners, residents etc. ☐ Defining the roles and responsibilities of the stakeholders

ID authorities need to ensure the registration/enrollment of every eligible citizen/legal resident in the country, so that a robust ecosystem of service delivery around the ID could be built. Hence, authorities need to actively engage partners and residents through various channels like radio, posters, social media etc. on an ongoing basis.

Institutional Structure

The institutional structure defined for an ID system is a critical factor in its successful implementation. This also has to include whether the ID agency is housed within government department or as an independent legal entity.

The illustration below outlines a typical institutional structure associated with a Government-run ID system is illustrated below:

FIGURE A.5 Institutional Structure

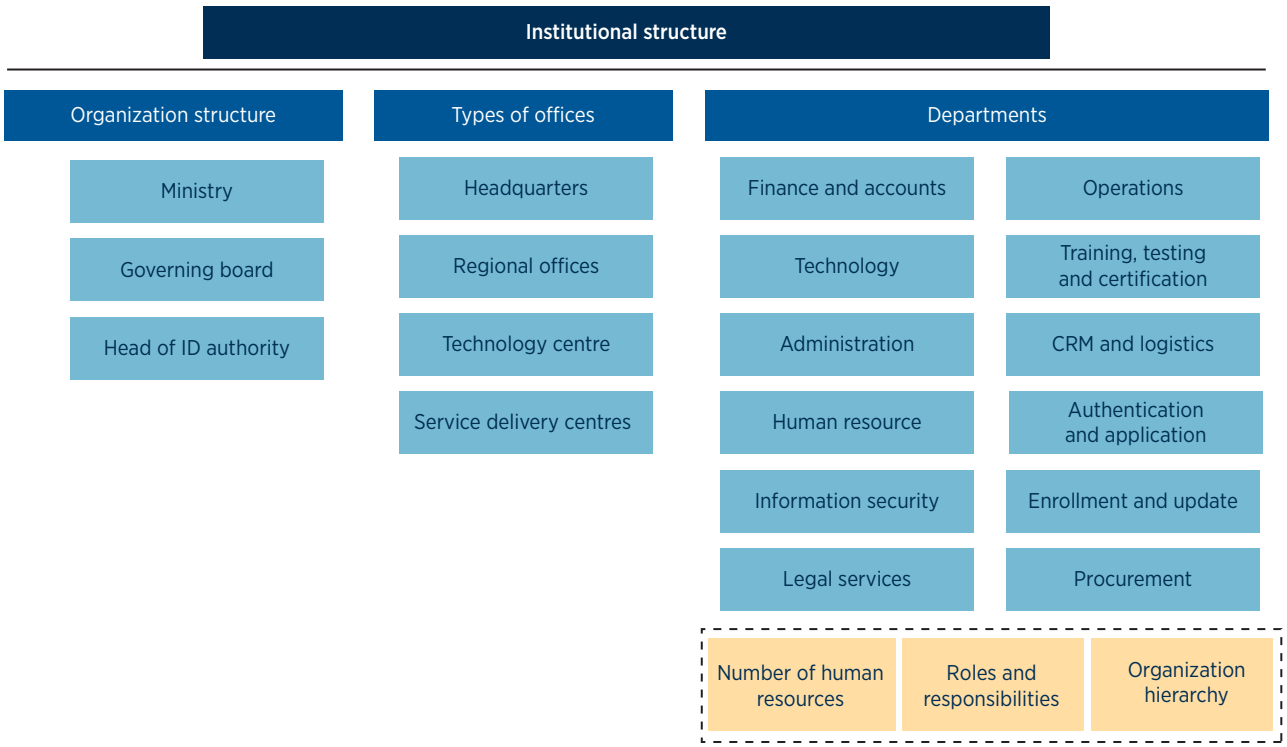
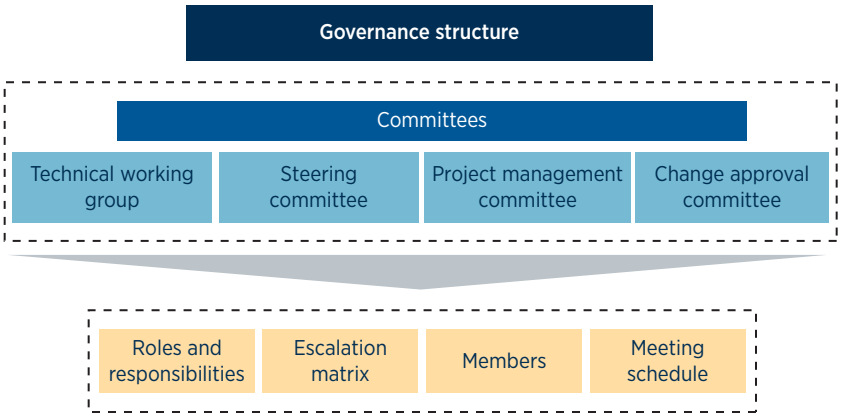


FIGURE A.6 Governance Structure



Architectural Governance

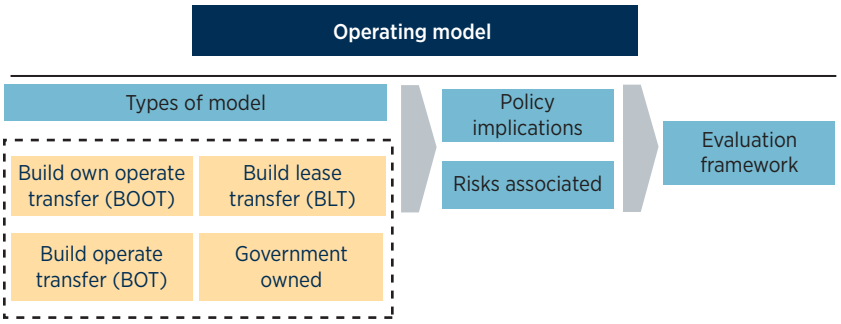
Architecture Governance shall play a key role in ensuring successful implementation of the ID system. It is expected that a strong governance structure shall assist the ID authorities and the service providers in fulfilling their roles and responsibilities in the program and ensure delivery of quality work products. This section describes the governance framework for an ID program. The broad level view of illustrative governance structure is illustrated in the diagram below:

Operating model

The operating model of an ID system adopted by a Government is another important factor that influences financial and operational arrangements to be used in the program. Operating model of the ID system demonstrates how the operations and services in the ID program are structured. An ID system is often capital cost-intensive and substantial costs are incurred in building and managing the technology infrastructure and services ecosystem. For a government (more so for governments in Lower Middle-Income Countries (LMIC) countries), the choice of program financing is critical to manage budget and to decide on the methods of building services (in-house/ in partnership etc.) The type of operating model is influenced by specific financing decisions, like reducing the upfront capital costs (as in a PPP-led ID system), or higher operational control (in a Government-run ID system, with its own staff). To balance overall program management and financing needs of ID systems, countries follow different operating models that address their program requirements adequately.

An ID system's operating model is typically influenced by the following elements as illustrated below:

FIGURE A.7 Overview of Operating Model



Business Model

Implementing an ID system in a country is a costly program which requires significant investments from the Government and other applicable program partners (e.g. private sector investment agencies in a PPP-based model). A critical requirement in the design of a "greenfield" ID system is the development of a sound "business model" for the ID authorities. This business model would typically involve the following components:

- Cost Model - Costs are incurred across the various phases of the program, right from the 'planning and design' phase to "implementation" phase as well as the ongoing "steady state" phase of the ID system.

Note: World Bank's ID4D group has developed a cost estimation model to assist countries in identifying the capital and operating expenditure incurred across the different phases of a greenfield ID system.

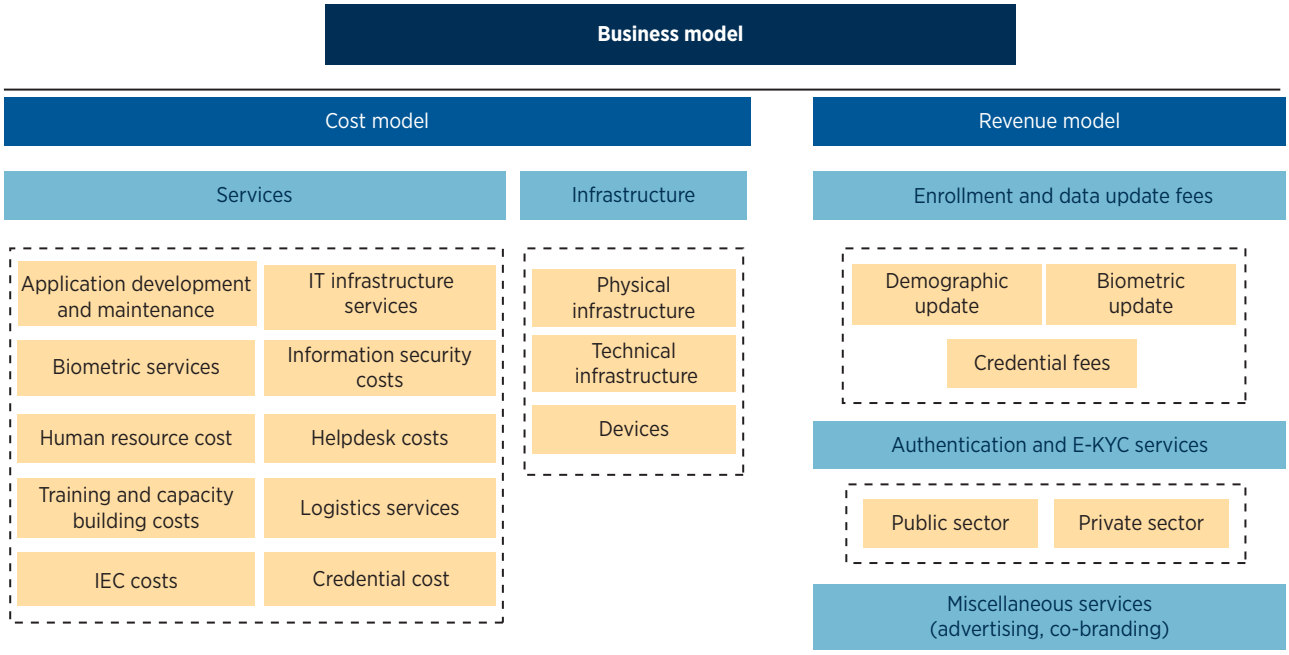
For more details, please refer "Reference cost model" and "Understanding Cost Drivers of Identification Systems"[1]

- Revenue Model – Some of the successful ID systems around the globe have also designed strong revenue models in order to make their ID systems 'fiscally sustainable' for the Government. Popularly seen revenue strategies include availing fees for specific services from enrolled citizens/residents and subscription-based fees from ID ecosystem partners in the public and private sector for specific ID-related services. Some of the them are:
  - Self- financed models like 'government funded', etc.
  - Self-sustaining financing models (charging the services provided)
  - Financed through a 'PPP' model such as BOT, BOOT, BOO etc.
  - International funding support like UNDP funded ID system in Malawi, World Bank in Morocco

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 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

[1] http://id4d.worldbank.org/Cost-Model

FIGURE A.8 Business Model



Note: For more details, please refer the documents on Public sector savings and revenue from ID systems[2] and Private Sector Economic Impacts from ID systems[3].

Typical procurement decisions in an ID system's business model are influenced by the following elements, as illustrated below:

Transition Strategy

This section intends to provide guidance to countries modernizing their legacy ID systems. ID authorities in such countries, periodically prioritize efforts to upgrade existing system capabilities (spanning across processes, services, applications and infrastructure), as well as to accommodate new services and modern technologies in the ID system. To support these activities, ID authorities need to undertake a detailed assessment of their legacy ID system capabilities and articulate policies and programmatic upgrades to meet their envisioned goals for a futuristic ID system. This assessment would also have to be accompanied by an implementation roadmap that would address the prevailing gaps and challenges faced by the existing ID system. The transition process and activities might include, but are not limited to, the following:

- Transition from existing system to new system
- From existing vendor to new vendor
- From paper based to new digitized system
- Upgrading the existing services and infrastructure
- Integration with Civil Registration System of the country

Technology Strategy

A strong technology backbone and a sound strategy for implementing the same will be vital for delivering the ID services to the residents and developing the identity ecosystem around it. As the enrollments in the ID system and the scope of services delivered through the ID system increases over time, the number of people authenticating themselves to use the services increasing exponentially and this calls for a strong technical infrastructure to support this.

[2] http://pubdocs.worldbank.org/en/745871522848339938/PublicSectorSavingsandRevenueIDSystems-Web.pdf

[3] http://pubdocs.worldbank.org/en/219201522848336907/PrivateSectorEconomicImpactsIDSystems-Web.pdf

The major sections within the technology design strategy includes:

A. Application Sub-system: Important applications such as enrollment system, authentication system customer relationship management etc. may be developed as per the latest emerging technologies. This section highlights the important applications which could be developed to support the ID system infrastructure, including:

1) Core applications such as enrollment, ID proofing, deduplication and authentication systems;
2) Supporting applications such as business intelligence systems, resident-focused mobile applications etc.

B. Technology infrastructure: This section highlights the necessary technical infrastructure like servers, network, storage etc. to operate the ID system.

C. Information security: With the increasing need to protect resident data and privacy, a strong information security architecture must be in place with necessary policies, security tools and infrastructure to ensure this.

D. Biometric system design: Biometrics may play an important part in an ID system as it accurately detects possible duplicates and improves the accountability, efficiency of the ID system, if the ID authority plans to enroll resident with biometrics. With ever increasing database size in the country and given the criticality of this component, it is important to design a robust system.

An ID system would need a technology refresh on an ongoing basis. The technology upgrade needs to be planned and emerging technologies should be carefully evaluated and adopted to improve the services and lower the cost of operations. However, ID authorities should ensure the design and architecture principles are compiled while doing the technological upgrade of the solution.

The ID system consists of technology components that require periodic upgrades to keep up with technological advancements made over time. Adoption of emerging technologies in technological areas such as - network, server, storage, application, biometric and operations – must be periodically prioritized during the phases of ID system. As the legacy technology infrastructure ages over time or reaches an “end of support” stage, ID authorities should plan and procure the appropriate technology available to enhance the capabilities of the ID system depending on the business requirements of the ID authority.

Typical procurement decisions in an ID system’s technology strategy are influenced by the following design elements, as illustrated below in the table:

Topic	Key decisions
Core Identity functions	☐ Enrollment/ data update client ☐ Enrollment backend application ☐ Issuance of Credential ☐ Authentication API depending on types of authentication decided ☐ Grievance redressal application and portals
Ancillary functions	☐ Administrative applications ☐ Knowledge management system ☐ Mobile application for residents ☐ Identity and access management system ☐ Document management system ☐ Analytics and Business Intelligence Module ☐ Testing and deployment module ☐ Fraud Management system ☐ Portals- Partners and public ☐ Logistics services ☐ IT monitoring and management systems

IT Infrastructure

The broad overview of the IT infrastructure ecosystem is illustrated in the following diagram:

Topic	Key decisions
Design	☐ Compute architecture ☐ Storage architecture Network architecture (Local and Wide Area Networks) ☐ Backup and Disaster Recovery architecture

Information security

The broad overview of the information security is illustrated in the following diagram:

Topic	Key decisions
Design	☐ Security for IT infrastructure such as database, storage, network, etc. ☐ Governance, risk and compliance framework including policy management, risk management, audits etc. ☐ Security operations infrastructure
Software	☐ Monitoring and management tools ☐ Security tools
Hardware	☐ Security Operations Infrastructure (SOC) infrastructure ☐ IT infrastructure for security

Biometric system design

One of the characteristics of the ID system is enroll residents and avoid duplicates. To ensure this, it is necessary that the resident's identity information which is captured is verified in the ID database to ensure no duplicates are entering the database. Additionally, biometrics enable easy authentication with high accuracy. Hence, it is beneficial for ID authorities to enroll residents with their biometrics for building an ID database without duplicates. ID authorities need to design the biometrics system to procure the required infrastructure and devices for the program. Multiple decisions like number of modalities, data standards need to be made. The key decisions which need to be taken are included in the table below:

Topic	Key decisions
Design decisions	☐ Number of modalities ☐ Type of biometric modalities ☐ Deduplication and manual adjudication process design ☐ Biometric systems performance o Identification and authentication accuracy figures (FPIR and FNIR) o Throughput time for de-duplication and authentication, o Response time for de-duplication and authentication ☐ Database sizing (size of raw image and template for modalities)
Biometric standards	☐ Data standards for different modalities ☐ Image acquisition standards ☐ Standards for quality control, compression, storage and templates ☐ Enrollment and authentication device standards

For more information on the biometric technology, please refer "Technology landscape[4]" and "Catalog of Technical Standards[5], ID4D Practitioners guide[6]"

The summary of technology-related procurement for an ID system is:

Service	Topic	Procurement (Services and Infrastructure)
Enrollment	**Software**	☐ Enrollment application ☐ API's for biometric data capture and quality checks
	Hardware	☐ Enrollment kit including desktops, printer, cameras, etc.
	Physical Infrastructure	☐ Setup of permanent and mobile centers ☐ Procurement model of centers (Rent/ Lease/ Own)
	Human Resources	☐ Staffing of resources at the enrollment stations ☐ Training of the resources
	Logistics	☐ Collection and Storage of validation documents ☐ Data transfer to ID authority
Data Update (Data management)	**Hardware**	☐ Data update kit ☐ Device specifications
	Software	☐ Data update client ☐ Quality assurance and fraud management system ☐ Document management system (if needed)
	Physical infrastructure	☐ Service delivery centers
Credential and issuance	**Software**	☐ Credential personalization and tracking ☐ Logistics portal for partners ☐ Self-print portal
	Hardware	☐ Printing infrastructure like printers, desktops, etc.
	Services	☐ Logistics partner
Authentication	**Software**	☐ Authentication APIs ☐ Risk prevention and fraud management systems
	Hardware	☐ Authentication infrastructure like desktops etc. ☐ Biometric capture devices ☐ IT infrastructure for offline authentication
Customer Relationship Management	**Software**	☐ Customer Relationship Management application ☐ Citizen/Resident facing websites, mobile apps ☐ Contact Center Software (Automatic Call Distribution (ACD), Interactive Voice Response System (IVRS)) ☐ Chatbots and Social Media plug-ins
	Hardware	☐ Contact Center Infrastructure
	Physical infrastructure	☐ Contact centers for Customer Relationship Management

(continued)

[4] http://pubdocs.worldbank.org/en/199411519691370495/ID4DTechnologyLandscape.pdf
[5] http://documents.worldbank.org/curated/en/707151536126464867/Catalog-of-Technical-Standards-for-Digital-Identification-Systems
[6] http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-Guide-Draft-for-Consultation.pdf

Service	Topic	Procurement (Services and Infrastructure)
Training, Testing & certification agency and content development agencies	**Software**	☐ Training software if required ☐ Testing and certification software for candidates undergoing training
	Physical infrastructure	☐ Training facilities
IT infrastructure		☐ Number and tier rating of data centers, including disaster recovery ☐ Ownership of data centers (e.g., owned, co-located, private cloud service providers) ☐ What type of software will be used (i.e., proprietary or open-source)

APPENDIX B
IMPLEMENTATION

This is the phase in which, the selected vendor(s) commence the design, development and deployment activities in the ID system implementation. The major components in this implementation phase include periodic monitoring activities to ensure compliance with requirements specified in the RFP(s).

The table below outlines key decisions and considerations to be addressed by ID authorities in this phase.

Topic	Key decisions
Monitoring and Compliance to requirements	☐ Monitoring and Evaluation framework to be defined for the services procured including but not limited to Biometric services, Infrastructure services, Application development and maintenance, Logistics, CRM etc. ☐ Process to ensure the conditions and scope of services defined in RFP o Monitoring the RFP project deliverables o Conformance to project timelines o Adherence to process and technical specifications o Monitor the Service level agreements o Processes to ensure the BOM deliverables as per the plan defined in RFP o Conformance to contractual conditions

APPENDIX C
STEADY STATE

The "steady-state" phase of the ID system life-cycle, includes processes that have to be followed by ID authorities, after a successful ID system implementation (as envisioned in the 'Plan and Design' phase). The major components of the steady-state phase include:

a. Monitoring and evaluation
b. Audit and compliance
c. Innovation
d. Transition (Vendor to the government and/or vendor to another vendor)

In the steady state, it is critical to have key monitoring processes in place to oversee assets and activity during this "steady state" phase (e.g. overall activity, quality of input data, performances including accuracy of biometric matching, dynamics in fraud patterns, grievances, etc.). Another benefit of this activity is that it helps ID authorities to better manage the transition and innovation components.

Once the contract period with the vendors comes to an end, ID authorities have to find the best way to ensure smooth contract renewals, without any service disruption. In this phase, an ID authority can add new services, enhance already existing services and procure cutting-edge infrastructure based on the needs and requirements of the ID system.

Monitoring and Evaluation

An effective and standardized monitoring and evaluation process will serve as a control mechanism for vendor(s) to deliver on the expected service levels, as outlined in the 'service level agreement' between both parties. The main objective is to improve overall effectiveness of the ID system by institutionalizing an approach to monitor and evaluate the effectiveness of services. It will also be used to learn how the system is being used in real life compared to the strategic expectations of the ID authority carried out in Phase – "Plan and Design". The monitoring and evaluation process will involve a periodic evaluation of enrollment processes, personnel and infrastructure to ensure quality, efficiency and effectiveness. ID authorities need to define KPIs for different services and processes in the scope of work, which would be measured against the actual performance of the vendor(s). This would help in a comparative and independent evaluation of the services provided by the vendor(s). Broadly put, a monitoring and evaluation framework will enlist who will monitor activities performed by the vendor(s) and outline the necessary actions to be taken in case the service levels are not met. Key considerations for ID authorities when defining such a framework, include the following:

- The ID authority should clearly define the complete end to end process, the frequency of measurement, and how the data around important program indicators would be collected.
- The ID authority should generate periodic reports for stakeholders implementing the ID system as well as for the governing body for tracking the outcomes of the ID program.
- The ID authority should the define success criteria for the ID implementation, against which the progress will be measured.

The table below outlines key decisions and considerations to be addressed by ID authorities:

Topic	Key decisions
Monitoring and Evaluation	☐ A 'Monitoring and Evaluation' framework to be defined for the services procured including but not limited to Biometric services, Infrastructure services, Application development and maintenance, Logistics, CRM etc. ☐ Processes to check compliance with legal and regulatory framework ☐ Parameters and methodologies for assessing various services provided by the bidder including but not limited to: o Throughput and response time o Scalability o Integration o Interoperability o Enrollment in a specific time period with average time for issuance o Biometric systems performance o Customer relationship management parameters like average response time, satisfaction matrix from the customers etc. ☐ Standards operating processes for monitoring and evaluation procedure ☐ Frequency for monitoring and evaluation reports

Audit and Compliance

Performing periodic compliance audits enable ID authorities to ensure a comprehensive review of the ID system's adherence to legal and regulatory guidelines. Audit reports generated through such audits can demonstrate the strength and thoroughness of compliance preparations, security policies, user access controls and risk management procedures, from time to time.

The table below outlines key decisions and considerations to be addressed by ID authorities.

Topic	Key decisions
Audit and Compliance	Procedure to ensure compliance to all laws applicable to ID system ☐ ID authority to encourage and enforce compliance with data protection laws and privacy laws ☐ Procedure and timelines for audit and compliance procedures ☐ Provision to ensure audit efficacy of the enrollment process to enroll residents ☐ Service under the authentication function to be audited and check for compliance ☐ Service level agreement (SLA) for audit and compliance to be defined ☐ Provision to incorporate inputs from audit and compliance procedures

Box C.1: Challenges faced in procurement for digital ID system by countries

A national development agency from a country in the Latin American and Caribbean region, faced an allegation that their contractor received preference during the procurement process. This led to an audit on whether the procurement of the national identity card and passport system was properly conducted in accordance with the proper regulations.

Innovation

ID authorities should strive to continuously introduce various innovations in the ID system, based on newer technology trends in the market, learnings from the past challenges faced, and so forth. As an important component in the steady state phase, the following considerations can be prioritized:

A. Developing a roadmap for short term and long-term goals – where the ID authority could clearly define its short term and long-term goals for the ID system.
   a. Short-term goals for the ID system might include efforts to add new services and improving the current services for the residents.
   b. Long-term goals might include efforts to transition completely to an open-source, open-standard, private cloud implementation or developing an in-house biometric solution for the ID system etc.

   ID authorities should include all the goals in their roadmap and continuously try to achieve them.

B. ID authorities should continuously seek to incorporate learnings from the challenges or roadblocks faced by them during the "procurement", and the "implementation" phases of the ID system lifecycle, as well look to incorporate learnings from other ID systems.

C. Services ecosystem - where ID authorities could add more services and continuously improve the services offered to the residents.

Transition

ID authorities need to manage various transitions during the ID system lifecycle. The termination of contracts for vendor(s) might result in a need to reformulate the strategy for procurement of ongoing services, addition of new services, or IT infrastructure.

The purpose of a "transition" stage is to:

A. Enable new vendors to transition and take over existing services from the incumbent vendors.

B. Enhance quality of services, optimize cost of operations and improve information security.

C. Increase services provided by the ID authority.

D. Help minimize disruption in services.

An ID authority should look at the existing contracts and post evaluation of the vendor(s). It may choose to do the following:

1. In-house development of services

   After the contract terminates for specific services, the ID authority has the option to develop the services in-house. The following points could be considered while taking the decision:

   a. The ID authority has developed the requisite expertise for delivering the services.

   b. The strategy is aligned with the architecture principles of the ID system and provide more independence to the ID authority.

2. Re-distribution of services to the various vendors

3. Upgrade of the IT infrastructure necessary for providing quality of services:

   a. Procurement and implementation of the similar proprietary systems

      In case the open source platforms are unable to meet the business requirements, the ID authority may have to continue with the proprietary products. Following are the pros and cons of adopting such an approach:

      i. Advantages: Best in class products can be sourced through competitive bidding to enable fitment of the solution vis-à-vis the business requirements. Better technical support can also be made available through the OEM partners.

      ii. Disadvantages:

         A. The products will be proprietary and can lead to an over-dependence on the OEM partner(s). Limitations of the OEM partner(s) could also be a disadvantage.

         B. Customization, integration and migration efforts may be curtailed.

   b. Transition to an open source system

      Often, vendor lock-in inhibits an ID authority's ability to adequately modernize a legacy ID system over time. Having a clear vision

on the need for a primarily open-source/ open standard driven technology stack will allow authorities enough flexibility to easily upgrade critical system components with lower vendor dependency. The open source solution should be evaluated on maturity of software and community, level of transparency, licensing type, guarantees in terms of maintenance and other liabilities. Also, since implementing an ID system often requires considerable technical expertise, embedding the right technical support requirements from vendors becomes an important procurement consideration for authorities.

i. Advantages will be;
   - A. No over-dependence on the OEM partner(s)
   - B. No product and technology lock-in
   - C. Better control over the system and product

ii. Disadvantages: ID authorities would need to source more in-house technical capacity to implement the open source solution.

APPENDIX D
KEY TERMS AND DEFINITIONS

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. In identification systems, common personal identity attributes include name, age, sex, place of birth, address, fingerprints, a photo, a signature, an identity number, date and place of registration, etc. [Source: Adapted from NIST (2013a)]

Authentication

The process of proving that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more "factors" or "authenticators" 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 is (e.g., their fingerprints), knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or does (e.g., their handwriting, keystrokes, or gestures). [Source: adapted from OWI (2017), NIST (2013a), World Bank 2016].

Usage:

- "Two-factor" authentication involves more than one of the factors described above (i.e., two things among what the person is, knows, have, and/or does).
- Although authentication and verification are related and often used interchangeably in the ID4D context, they can be distinguished by whether the process involves determining the veracity of particular attributes or credentials (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.

Biometric characteristic

A biological (fingerprint, face, iris) or behavioral (gait, handwriting, signature, keystrokes) characteristic 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).

Usage:

- Biometric identification is often used to deduplicate identity records during or after enrollment (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).

Usage:

- Biometric verification is used during authentication procedures (i.e., a 1:1 match of a captured biometric template against one stored on a card or in a 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).

Credential

A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. The 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. [Source: adapted from World Bank (2016, 2018b)].

Usage:

- The identity "credential" is preferred to identity "document" in most contexts, as it is more encompassing, and many digital credentials are not physical documents.

Deduplication

In the context of identification systems, deduplication is a technique to detect duplicate identity records. Biometric data—including fingerprints and iris scans—is commonly used to perform a duplicate biometric enrollment check to identify false or inconsistent identity claims and to establish uniqueness (adapted from ISO/IEC 2382-37 and World Bank (2018b)].

Digital identity

A set of electronically captured and stored attributes and/or credentials that uniquely identify a person. [Source: adapted from World Bank (2018b), EC (2017), IDB (2013)].

Usage:

- The term "digital identity" is commonly used when referring to a person's digital identity, whereas the term "digital ID" when referring to a digital identity credential or system.
- A 'digital identity' is synonymous with "electronic identity" in most ID4D contexts.

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. [Source: adapted from World Bank 2016].

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. [Source: NIST SP800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf]

Electronic signature

An electronic authentication technique that carries the legal weight of—and substitutes for—a handwritten signature. [Source: Adapted from UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001.]

Usage:

- Note that "electronic signature" and "digital signature" 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 serve the same purpose as an electronic signature (which is specifically to substitute for a handwritten signature).

Foundational identification (ID) system

An identification system primarily created to provide general identification and credentials to the population for public administration and a wide variety of public and private sector transactions, services, and derivative credentials. Common types of foundational ID systems include civil registries, national IDs, universal resident ID systems, and population registers. [Sources: adapted from World Bank (2018a, 2018b), Gelb & Clark (2013)].

Usage:

- Countries typically have multiple foundational ID systems that may not be entirely distinct. For example, one country may have a population register linked to the civil registration system that is used both to generate 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 status and issuing government-recognized credentials.
- The distinction between foundational and functional ID systems is about the purpose for which they were created. For example, functional credentials (e.g., driver's licenses or social security numbers in the U.S.) that serve as the primary means of identification and authentication for a variety of purposes, should not be considered foundational ID systems. Some countries, however, have built foundational ID systems based on functional systems (e.g., Bangladesh).

Functional identification (ID) system

An identification system created to manage the identity lifecycle 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. [Sources: adapted from World Bank (2018a, 2018b, 2016), Gelb & Clark (2013)].

ID

1. Identity document (see 'Credential').
2. 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 (e.g., "national ID card" rather than "national ID") in order to avoid ambiguity where appropriate.

Identification

The process of establishing, determining, or recognizing a person's identity. [Source: adapted from World Bank (2018)].

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, credentials, and legal frameworks associated with the capture, management, and use of personal identity data for a general or specific purpose. [Source: adapted from World Bank (2017)].

Usage:

- Use "identification/ID system" instead of "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 identify a person. [Source: World Bank (2017, 2018b)]

Identity document (ID)

An identity credential. See also "ID".

Identity ecosystem

The set of identification systems—including databases, credentials, laws, processes, protocols, etc.—and their interconnections within a geographic area or particular sector. [Source: adapted from World Bank 2016].

Identity lifecycle

The process of registering, issuing, using and managing personal identities, including enrollment of identity data; validation through identity proofing and deduplication; issuing credentials; verification and authentication for transactions; and updating and/or revoking identities and credentials. [Source: adapted from World Bank (2016)].

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. [Source: adapted from NIST (2015, 2017)].

Identity provider

The entity—e.g., a government agency or private firm—with primary responsibility for issuing and managing identities and credentials throughout the identity lifecycle. [Source: adapted from World Bank (2016)].

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).

(Level of) identity assurance (LOA)

The ability to determine, with some level of certainty or assurance (LOA), that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity. [Source: World Bank 2016].

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 citizenship 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 nationwide 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 administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. [Source: NIST SP800-63-3: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf]

Population registers

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.

Proof of legal identity

Government-recognized credentials—such as birth certificates, identity cards, and unique identity numbers—that serve as proof of legal identity in accordance with national law, irrespective of whether they also serve as proof of citizenship. [Pending HLAC/UN definition]

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). [Source: adapted from IDB (2013)].

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—for their lifetime. UINs are typically assigned after validating a person's identity and statistical uniqueness through a process such as biometric deduplication. [Source: adapted from World Bank (2016)].

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 citizens and non-citizens.

Usage:

- NID systems may be universal resident ID systems to the extent that they are digital and provide IDs to legal residents as well as citizens.

Verification

The process of verifying identity attributes or determining the authenticity of credentials in order to facilitate authorization for a particular service. [Source: adapted from World Bank (2018a)].

Usage:

- Although authentication and verification are related functions and often used interchangeably, they can be distinguished by whether the process involves determining the veracity of attributes or credentials (verification) or ensuring that a person is who they claim to be (authentication)

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.

id4d.worldbank.org

ID4D
IDENTIFICATION FOR DEVELOPMENT