UNIQUE IDENTITY (UID) SYSTEM

STRATEGIC PLAN | 2021 TO 2025

MAY 2021

VOLUME I

TRUSTED DIGITAL IDENTITIES TO UNLOCK SERVICES FOR ALL

EXECUTIVE SUMMARY

This document describes the Government's strategy to create Unique IDs in Timor-Leste. The Unique ID will establish a digital identity, consisting of a minimum set of data including a random unique number, biographical data (name, date of birth, etc.) and biometric information. Biometric data will prevent duplicate registration for services.

The system will enable citizens and residents to more reliably access a wide range of public and private services. It will also help the private sector and Government to reduce fraud and fake identities and to cut transaction costs in verifying identity. International studies show that identity systems can significantly support economic growth and access to financial services.

This strategy covers the 2021 to 2025 period. By 2025, we intend to register 1 million persons and to link digital identities to the banking and telecoms sectors, voter and civil registration, health and education records, business registration, and several other key functional databases. The databases already collect personal information on citizens and residents. The required investment (to be funded through CAFI, donor resources, and the recurrent budget) is expected to reach $US 13.8 Million. The project is calculated to have an internal rate of return of 24% when using a 15-year time horizon, making it extremely favorable. The project is expected to deliver net benefits (in excess of costs) of $US 12.9 Million over this period.

In creating a unique digital ID, citizens' data and privacy will be strongly protected, consistent with Article 38 of the Constitution. A *Data Privacy and Protection Law* has been drafted to ensure these rights. The law will include limits on data collection and access, user control over data, user choice on whether to enroll or to use the Unique ID (i.e. voluntary rather than compulsory enrollment) and the establishment of independent and effective grievance redress mechanisms.

The Unique ID system will also support the upgrade of civil registration processes and data management under the mandate of the Ministry of Justice. In the future this will better link digital and civil identity.

This strategy and operational plan was developed in-house by the Government, using a consultative process, by a Technical Committee led by the Presidency of the Council of Ministers, the Ministry of Justice, and TIC Timor. The Ministries of Health, Education, Finance, Interior, State Administration, Social Solidarity and Inclusion, and the Civil Service Commission directly participated. In the process, options were presented, debated, and mutually agreed upon within the Council of Ministers.

This strategy benefitted from the high quality and timely technical and financial support that was provided by the UNDP, UNICEF, and the World Bank. It greatly benefited from the direct sharing of experiences in India, the Philippines, Cape Verde, and Estonia.

It is time now to implement these important changes. The success of the Unique ID will depend on the ongoing cooperation of all relevant Ministries, the private sector, and citizens in improving access to essential services throughout Timor-Leste.

FEEDBACK

The Government of the Timor-Leste welcomes comments and feedback to improve the design and implementation of this strategic plan. We urge citizens, civil society organizations and other interested partners and stakeholders to contact us and to discuss any matter of interest raised by our plan. Please assist us by letting us know what you think and identifying ways for us to work together and to improve the services we deliver.

Phone

+670 7712-5077

Email

info@uid.gov.tl

Web Site

www.uid.gov.tl

Social Media

https://www.facebook.com/tictimor/

Written Correspondence

Unique ID Secretariat
TIC Timor
Palacio do Governo
Dili, Timor-Leste

TABLE OF CONTENTS

Contents

Executive Summary ... i
Feedback ... ii
Table of Contents ... iii
Abbreviations ... vi
Glossary of Terms ... vi
Tables and Figures ... viii
Overview ... 1
Introduction ... 1
Vision ... 2
Objectives ... 3
Implementation Principles ... 3
Creating this strategic plan ... 4
Current Situation ... 4
Civil Identity ... 6
Other Systems and Identity Cards ... 6
Options ... 7
Assessment of the available options ... 7
Option 1: Separation -Birth Certificate Optional ... 7
Option 2: Joint Registration – Birth Certificate Required ... 8
Option 3: A single registry, with digital identity integrated into the Civil Registry ... 8
Option 4: One column approach ... 8
Phases and program overview ... 9
Risks and risk mitigation ... 11
Layout ... 11
Expected Results ... 11
Component 1: Legal and institutional foundations ... 13
Introduction ... 13
1.1 Develop, finance, and complete procurement for a UID project ... 13
1.2 Create laws to protect citizens' data and privacy ... 14
1.3 Strengthen the legal environment surrounding Unique ID ... 14
1.4 Establish a UID Mission structure ... 15
Results ... 15
Component 2: UID system development ... 17
Introduction ... 17
Component overview ... 17
2.1 Procure Software and Equipment ... 18
2.2 Customize and operationalize UID Software ... 18
Functionality ... 18
System architecture ... 19
Privacy ... 20
Security ... 20
Scalability and manageability ... 20

UID Cards ... 20
2.3 Establish UID security and privacy Protocols ... 20
2.4 Standards and Data Exchange Protocols ... 21
2.4 DMIS enhancement and BI cards ... 21
Civil registration and vital statistics (CRVS) software ... 22
BI Cards ... 22
Results ... 23
Component 3: UID Registration & validation ... 24
Introduction ... 24
Component overview ... 25
3.1 Registration logistics and partnerships ... 25
Planning for Suco Registration ... 25
Registration by Government agents: Rural Sucos ... 26
Registration by approved agents: Urban and Semi-Urban Sucos ... 26
Training ... 27
Help line ... 27
Consultation ... 27
3.2 Implement Registration of 1 million persons ... 27
3.3 Validation and credentials ... 28
BI Cards and the Ministry of Justice ... 28
3.4 Expand and upgrade birth registration ... 28
Results ... 29
Component 4: use cases and Functional databases ... 30
Introduction ... 30
Component overview ... 31
4.1 UIN WITHIN Payments Databases (Group I) ... 32
4.2 UIn within MOJ and MOH databases (group II) ... 32
4.3 UIN Within the voter ID database (group III) ... 33
4.4 UIN Within education and Other Ministries (group iV) ... 33
Results ... 33
Component 5: outreach and communications ... 35
Introduction ... 35
Component overview ... 35
5.1 Launch and brand UID to gain government commitment ... 36
5.2 Facilitate debate on and disseminiation of privacy and data protection to build the trust of potential users ... 36
5.3 Motivate citizens to register for a unique id ... 37
5.4 Motivate public and private entities to incorporate UID into their functional databases ... 37
Results ... 38
Summary budget ... 39
Annex 1: Pros and cons of the 4 options ... 41
Annex 2: Organizational structures ... 45
From project to mission structure to agency ... 45
Continue governance arrangement under the Technical Committee ... 45
Begin operations in a project mode, closely associated with TIC ... 46
Undertake procurement ... 46
Develop a financing strategy for the Agency ... 46

Seek technical assistance from development partners to support operations 46
Steady state operations 47
Transition to a long term organizational structure 47
Annex 3: UID and DMIS systems requirements 48
Introduction 48
UID Software and Equipment 48
Functionality 48
Civil registration (DMIS) software and equipment 56
DMIS / Electronic Civil Registry Functionality 56
Annex 4: Registration 57
Introduction 57
Registration logistics and partnerships 57
Registration 59
Develop registration procedures and processes 59
Identify, select and regulate external enrolment agencies and internal registrars 59
Develop hardware and software standards and require and certify their use 60
Train registration staff 60
Registration monitoring and continuous improvement process 60
Annex 5: Security 61
Introduction 61
Main Principles 61
Annex 6: cost benefit analysis 64
Costs 64
Definition of Benefits 64
Functional Databases generate the benefits 65
Calculating benefits of the UID 65
IRR Calculations and sensitivity analysis 66
Annex 7: Activity plan and schedule 67
Annex 8: Detailed budget 72

ABBREVIATIONS

BI, Billete Identidadi

CRVS, Civil Registration and Vital Statistics

DB, Database

DMIS, Demographic Management Information System

DOB, Date of Birth

HR, Human Resources

GDS, General Directorate of Statistics

ICT, Information and Communication Technology

ID, Identifier or Identification

IEC, information, education, communication

M&E, Monitoring and Evaluation

MIS, Management Information System

MOE, Ministry of Education

MOH, Ministry of Health

MOJ, Ministry of Justice

MRLAP, Ministry of Legislative Reform and Parliamentary Affairs

MSSI, Ministry of Social Solidarity and Inclusion

MNLCA, Ministry for National Liberation Combatants Affairs

MTC, Ministry of Transport & Communication

NCIS, National Criminal Investigation Service

NCBTL, National Commercial Bank Timor-Leste

POB, Place of Birth

RDTL – República Democrática de Timor-Leste

SAII: Support for The Elderly and Invalids

STAE – Secretariado Técnico de Administração Eleitoral

SP, Strategic Plan

TIN, Taxpayer Identification Number

TL, Timor-Leste

UID, Unique Digital Identification, Unique Digital Identifier

UIN, Unique Identifier Number

UNDP, United Nations Development Programme

UNICEF, United Nations Children's Fund

GLOSSARY OF TERMS

Authentication, [1] the process of establishing confidence that a person is who they claim to be. Digital authentication generally involves a person electronically presenting one or more "factors" to "assert" their identity—that is, to prove that they are the same person to whom the identity or credential was originally issued. These factors can include something a person knows (e.g., a password or PIN), has (e.g., an ID card, token, or mobile SIM card), or is (e.g., their fingerprints)

API, Application Programming Interface is a software intermediary that allows two applications to talk to each other.

Biographic data, refers to attributes about a person or their life, that are not biometric (i.e., biological or behavioral). In this UID system this includes information such as name, date of birth, place of birth, parents' names. Same as **Demographic Data.**

Biometric data, a biological (fingerprint, face, iris, voice) or behavioral (gait, handwriting, signature, keystrokes) attribute of an individual that can be used for biometric recognition. This is individual to each person, and can be used to deduplicate identity records during registration, or for biometric verification used during authentication procedures to conduct a 1:1 match of the person.

Barcode is a square or rectangular image consisting of a series of parallel black lines and white spaces of varying widths that can be read by a scanner. **Barcodes** are applied to products as a means of quick identification.

Civil identity, the basic characteristics of an individual's identity (e.g. name, sex, place and date of birth), conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death.

[1] Terms are based on the" Practitioners Guide" World Bank Group Identification for Development https://id4d.worldbank.org/guide/glossary

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 requirement in each country. Civil registration is carried out primarily for the purpose of establishing the documents provided by the law

Closed source software is software that holds the source code safe and encrypted. Meaning, the user cannot copy, modify, or delete parts of the code without some type of consequence. It allows users to copy, modify, or delete parts of the code under their own discretion.

Credential, A document, object, or data structure that vouches for the identity of a person through some method of trust and authentication. Common types of identity credentials include—but are not limited to—ID cards, certificates, numbers, passwords, or SIM cards. A biometric identifier can also be used as a credential once it has been registered with the identity provider.

Digital identity is a collection of electronically captured and stored identity attributes that uniquely describe a person within a given context and are used for electronic transactions. A digital identity system refers to the systems and processes that manage the lifecycle of individual digital identities. A person's digital identity may be composed of a variety of attributes, including **biographic data** and **biometric data** (e.g., fingerprints, iris scans, hand prints) as well as other attributes that are more broadly related to what the person does or something someone else knows about the individual. When these data are collected and verified, they can be used to identify a person by answering the question "who are you?". These attributes, along with credentials issued by the service provider (e.g., unique ID number, eDocument, eID, mobile ID) can then also be used as **authentication factors** to answer the question "are you who you claim to be?". The attributes and authentication factors used in a digital identity may vary from one context or country to the next depending on the type of identity system. Digital identities are created and used as part of a lifecycle that includes three fundamental stages: (a) registration, including enrollment and validation, (b) issuance of documents or credentials, (or certificates) and (c) authentication for service delivery or transactions.

eDocument, electronic Document is a computerized document that is used to record information and provides for the easy and instant processing of information.

E-Government, the application of Information and Communication Technologies to government functions and procedures with the purpose of increasing efficiency, transparency and citizen participation

eID, electronic Identification is a digital solution for proof of identity of citizens or organizations. It can be used to view the access benefits or services provided by government authorities, banks, or other companies, for mobile payments, etc. One form of **eID** is an **electronic identification card** (eIC), which is a physical identity card that can be used for online and offline personal identification or authentication.

Foundational ID, or Registry, or database, an identification system primarily created to manage identity information for the general population and provide credentials that serve as proof of identity for a wide variety of public and private sector transactions and services. This is the same as a UID System in this context.

Functional ID, or Registry, or database, a system created in response to a demand for a particular service or transaction, which may issue identity card or token such as IDs, drivers licenses, health and insurance records, bank cards, etc. These may be commonly accepted for broader identification purposes, but may not bestow full legal identity

GIS, Geographic Information System is a framework for gathering, managing, and analyzing data. Rooted in the science of geography, GIS integrates many types of data. It analyzes spatial location and organizes layers of information into visualizations using maps and 3D scenes.

ISO, International Organization for Standardization is an independent, non-governmental, international organization that develops standards to ensure the quality, safety, and efficiency of products, services, and systems.

Know Your Customer (KYC or e-KYC) are guidelines in financial services requiring an effort to verify the identity, suitability, and risks involved with maintaining a business relationship. The procedures fit within the broader scope of an entities Anti-Money Laundering (AML) policy

Level of assurance (LOA), the ability to determine, with some level of certainty or assurance, that a claim to a particular identity made by some person or entity can be trusted to actually be the claimant's "true" identity.

Mobile ID refers to a user's digital identity, and the technology used to manage it, in the hyper-connected world of smartphones, tablets, wearable technology and the Internet of Things.

NIST, National Institute of Standards and Technology is based on best practices from several security documents, organizations, and publications, and are designed as a framework for federal agencies and programs requiring stringent security measures.

Open-source software is any computer software that is distributed with its source code available for modification. That means it usually includes a license for programmers to change the software in any way they choose: They can fix bugs, improve functions, or adapt the software to suit their own needs.

OTP, One-time-password SMS is a secure authorization method where a numeric or alphanumeric code is sent to a mobile number. This password is an added layer of security used to verify the identity of a user logging into an online platform, application, or website.

PKI, Public Key Infrastructure enables users of a basically unsecure public network such as the Internet to securely and privately exchange data using a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

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

QR, **Quick Response code** is a type of barcode that can be read easily by a digital device and which stores information as a series of pixels in a square-shaped grid. QR codes are frequently used to track information and allow the user to access information instantly.

Smart ID Card, a card that can facilitate digital authentication using appropriate technologies, such as a QR/bar code or integrated chip

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

UID, Unique Identity System, the system managing digital identity

UIN, Unique Identifying Number, a number that uniquely identifies a person—i.e., each person only has one UIN and no two people share the same UIN. UINs are generally assigned for a person’s lifetime (i.e., their number does not change over time), typically after validating a person’s identity and uniqueness through deduplication process. It is a number that can be used to link an identity across databases and systems in both the public and private sector

Vital statistics is accumulated data gathered on live births, deaths, migration, fetal deaths, marriages and divorces. The most common way of collecting information on these events is through civil registration, an administrative system used by governments to record vital events which occur in their population.

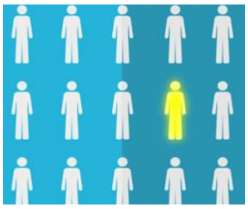
TABLES AND FIGURES

TABLE 1: TECHNICAL STEERING COMMITTEE....4
TABLE 2: IDENTITY AND CERTIFICATE SYSTEMS THAT COULD BE LINKED TO UID....5
TABLE 3: OVERVIEW OF THE 5 PROGRAM COMPONENTS....9
TABLE 4: KEY RESULTS....12
TABLE 5: COMPONENT #1 EXPECTED RESULT....15
TABLE 6: COMPONENT #2 EXPECTED RESULTS....23
TABLE 7: POSSIBLE REGISTRATION INCENTIVES....26
TABLE 8: COMPONENT #3 EXPECTED RESULTS....29
TABLE 9: STEPS IN THE PROCESS OF LINKING UID TO FUNCTIONS DATABASES....31
TABLE 10: ROLLOUT PLAN FOR EACH GROUP (IMPLEMENTING STEPS 1 TO 6)....31
TABLE 11: GROUP I PROJECTIONS FOR NUMBER OF RECORDS VERIFIED....32
TABLE 12: GROUP II PROJECTIONS FOR NUMBER OF RECORDS VERIFIED....32
TABLE 13: GROUP IV PROJECTIONS FOR NUMBER OF RECORDS VERIFIED....33

TABLE 14: COMPONENT #4 EXPECTED RESULTS 33
TABLE 15: COMPONENT #5 EXPECTED COMMUNICATION RESULTS 38
TABLE 16: PROJECTED COSTS BY MAIN CATEGORY (ALL YEARS) 39
TABLE 17: PROS AND CONS FOR OPTION #1 (SEPARATE DIGITAL AND CIVIL IDENTITIES) 41
TABLE 18: PROS AND CONS FOR OPTION #2 (JOINT REGISTRATION) 42
TABLE 19: PROS AND CONS FOR OPTION #3 (ALL WORK UNDER THE DMIS) 43
TABLE 20: PROS AND CONS FOR OPTION #4 (ONE COLUMN) 44
TABLE 21: DATA COLLECTION AND REGISTRATION REQUIREMENTS 50
TABLE 22: DATA COLLECTION AND REGISTRATION REQUIREMENTS 51
TABLE 23: ADMINSITRATION REQUIREMENTS 52
TABLE 24: REQUIREMENTS FOR CREDENTIAL PRODUCTION AND DISTRIBUTION 53
TABLE 25: REQUIREMENTS FOR VERIFICATION SERVICES 54
TABLE 26: REQUIREMENTS FOR VERIFICATION SERVICES 55
TABLE 27: REQUIREMENTS FOR AN IMPROVED COMPUTERIZED CIVIL REGISTRY SYSTEM 56
TABLE 28: PRINCIPLES OF AN INCLUSION STRATEGY 57
TABLE 29: TYPES OF BENEFITS OF THE UID 64
TABLE 30: PROJECTED NUMBER OF RECORDS IN DIFFERENT FUNCTIONAL DATABASES 65
TABLE 31: SENSITIVITY OF THE IRR UNDER DIFFERENT ASSUMPTIONS 66
TABLE 32: DETAILED BUDGET (TOTAL ACROSS ALL YEARS) 72

FIGURE 1: SOME KEY TERMS USED 1
FIGURE 2: DIGITAL VS CIVIL IDENTITY 1
FIGURE 3: UNIQUE ID OVERVIEW 2
FIGURE 4: OPTIONS FOR UID SYSTEMS 7
FIGURE 5: OVERVIEW OF THE STRATEGIC PLAN / PROJECT 10
FIGURE 6: EXPECTED PRINCIPLES ON DATA PRIVACY 14
FIGURE 7: IDENTITY AND DIGITAL IDENTITY 15
FIGURE 8: DESIGN PRINCIPLES OF THE UID SYSTEM 17
FIGURE 9: BUILDING BLOCKS OF ID SYSTEMS 18
FIGURE 10: KEY FUNCTIONALITY OF THE UID SYSTEM 18
FIGURE 11: KEY MODULES 20
FIGURE 12: DMIS SOFTWARE CONSTRAINTS 21
FIGURE 13: PRINCIPLES OF UID REGISTRATION 24
FIGURE 14: TYPICAL REGISTRATION EQUIPMENT 25
FIGURE 15: EXPECTED CUMULATIVE NUMBER OF PERSONS REGISTERED 28
FIGURE 16: EXPECTED CUMULATIVE % OF THE POPULATION REGISTERED 28
FIGURE 17: UID AS A CENTRAL REPOSITORY OF DIGITAL ID DATA 30
FIGURE 18: TARGETED BACKLOG OF PAPER CIVIL REGISTRY RECORDS TO BE ENTERED INTO THE DMIS 32
FIGURE 19: COMMUNICATIONS PRINCIPLES 35
FIGURE 20: LAUNCHING 36
FIGURE 21: DATA PROTECTION 36
FIGURE 22: REGISTRATION 37
FIGURE 23: FUNCTIONAL DATABASES 37
FIGURE 24: COST COMPOSITION 39
FIGURE 25: KEY STEPS IN FORMING AN AGENCY 45
FIGURE 26: COMPONENT #2 GOAL AND OUTPUTS 48
FIGURE 27: NECESSARY MODULES AND FUNCTIONALITY OF THE UID SOFTWARE 49
FIGURE 28: COMPONENT #3 GOAL AND OUTPUTS 57
FIGURE 29: KEY REGISTRATION STEPS 59
FIGURE 30: NUMBER OF RECORDS IN ALL FUNCTIONAL DATABASES 65
FIGURE 31:COMPOSITION OF BENEFITS 66

OVERVIEW



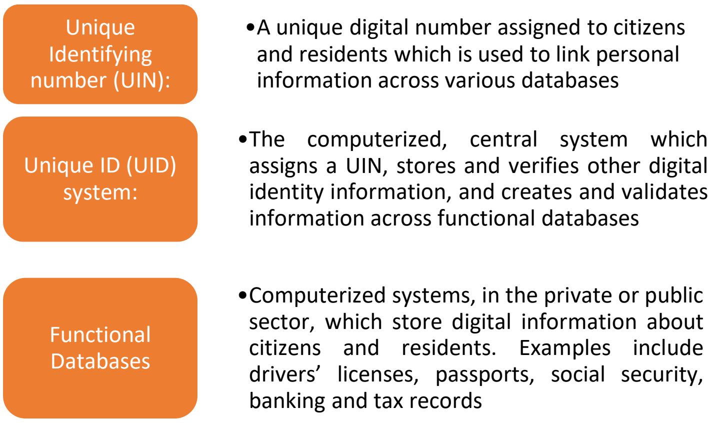
INTRODUCTION

This strategic plan defines a broad direction forward for the Government of Timor-Leste to create a digital system of unique identification (UIDs), for its citizens and residents. The plan covers 5 years from January 2021 to December 2025. It is supported by a more detailed operational plan and budget (Volume II) and in the future will be financed through a mixture of GoTL funding via CAFI and the Development Partners in a UID project managed under a Mission Structure.

A UID (digital identity) differs from a civil or legal identity. A UID is solely concerned with establishing reliable access to digital services and digital information. *In a digital environment*, the system of unique IDs[2] helps:

- **Identification** ("Who are you?") Determines digital identity by collecting and proofing information about the person. The UID system will *register* an individual and issue *credentials* that allow the individual to assert their identity
- **Authentication** ("Are you who you claim to be?") Checks that the person asserting the identity is the true owner of the identity based on what they have, what they know or who they are
- **Authorization** ("Are you authorized or eligible for something?") Allows relying parties, like Ministries and Banks, to provide access to services by verifying uniqueness of identity.

FIGURE 1: SOME KEY TERMS USED

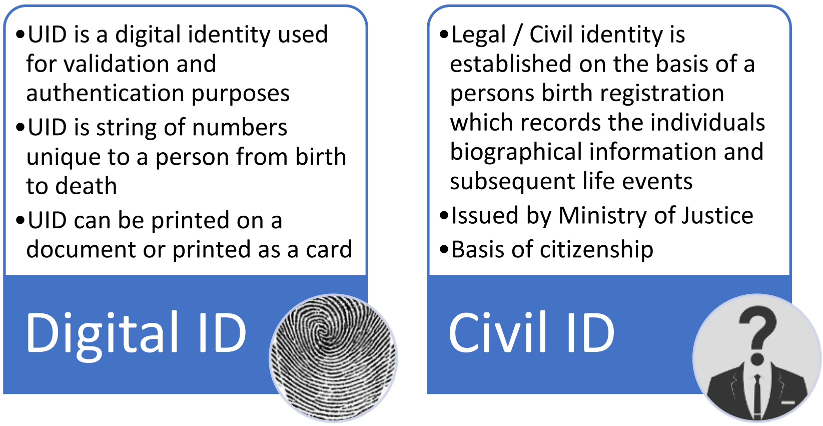


Unique Identifying number (UIN):
- A unique digital number assigned to citizens and residents which is used to link personal information across various databases

Unique ID (UID) system:
- The computerized, central system which assigns a UIN, stores and verifies other digital identity information, and creates and validates information across functional databases

Functional Databases
- Computerized systems, in the private or public sector, which store digital information about citizens and residents. Examples include drivers' licenses, passports, social security, banking and tax records

FIGURE 2: DIGITAL VS CIVIL IDENTITY



Digital ID
- UID is a digital identity used for validation and authentication purposes
- UID is string of numbers unique to a person from birth to death
- UID can be printed on a document or printed as a card

Civil ID
- Legal / Civil identity is established on the basis of a persons birth registration which records the individuals biographical information and subsequent life events
- Issued by Ministry of Justice
- Basis of citizenship

The UID system will do identification and authentication as its two core functions. This will help with delivering services, exercising rights, savings government funds, and enabling digitalization (especially of services, data and payments) but the relying parties will be doing authorization. And within the limits to be established by the Data Privacy and

[2] Based on the World Bank's "Practitioner's Guide" (2019), page 11.

Protection law, it can be used by the State to deliver benefits to targeted individuals and reduce, if not eliminate, fakes, duplicates and ghosts in beneficiary lists.

In the UID system, a digital identity, stored in a central secure database, for each individual, will consist of:

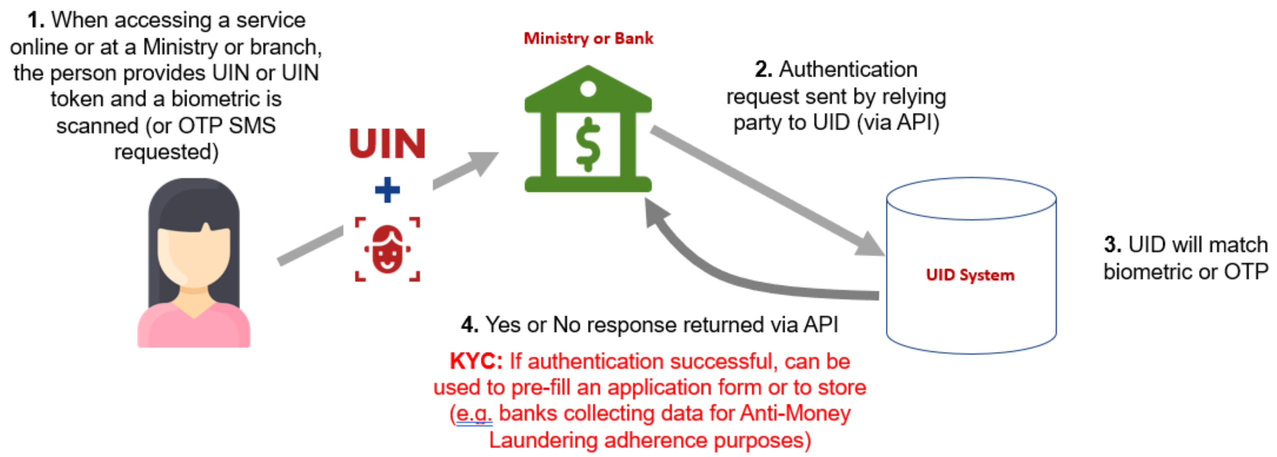
1. A randomly-generated **unique ID number** (UIN) to individually identify a person. The UIN will link the information contained in other electronic databases, as a key to enable 1:1 search for authentication.

2. A minimum set of **biographical information**, such as name, date of birth, place of birth, that will be collected during the registration process.[3] This information will be enough to help relying parties meet their identity proofing and compliance needs for key use cases, such as applying for government services and payments and opening a bank account.

3. **Biometric information**, such as facial image, fingerprint data, and possibly iris data, for persons over 13 years of age[4], to establish the uniqueness of individuals and facilitate secure authentication of their unique identity.

Therefore, a Unique ID will use a minimum set of digital data establishing a digital identity and used to access digital services, to link digital data across systems, and to ensure the integrity and uniqueness of digital information. It is not only an identity card and it is not necessarily a legal or civil identity. There will be linkages between Digital and Civil Identity over time, when UID links to Birth Records, which does provide legal identity. While biometric information is sufficient to de-duplicate and assign a unique ID to individuals, the biographical information will be used for Know Your Customer (KYC) purposes, such as opening a bank account or applying for a service or functional ID.

FIGURE 3: UNIQUE ID OVERVIEW



1. When accessing a service online or at a Ministry or branch, the person provides UIN or UIN token and a biometric is scanned (or OTP SMS requested)

2. Authentication request sent by relying party to UID (via API)

3. UID will match biometric or OTP

4. Yes or No response returned via API

KYC: If authentication successful, can be used to pre-fill an application form or to store (e.g. banks collecting data for Anti-Money Laundering adherence purposes)

VISION

Our vision is:

All people have trusted digital identities unlocking access to services

[3] As discussed later, other information will be collected for children.

[4] UNICEF, July 2019. "Faces, Fingerprints & Feet. Guidance on assessing the value of including biometric technologies in UNICEF-supported programs"

OBJECTIVES

The Unique ID system aims to improve access and delivery of Public and Private services to all people, citizens and residents, and to assist the Government to better manage these services. Transactions are expected to increasingly be online over time.

The objectives of UIDs are:

People's benefits

1. To increase convenience and **access** to services
2. To expand the **range of services** received
3. To improve the **quality, reliability and speed** of services received
4. To ease access to the formal banking and financial sector, **promoting financial inclusion and mobile banking**
5. To **provide a form of identity** to those currently unacknowledged by government and society
6. To enable people **to monitor and control** how their personal data is used and shared between service providers

Government benefits

1. To provide a better overview of all people residing in Timor-Leste, greatly **improving state planning**
2. To reduce **fraud**, fake and duplicate identities; to stop leakage and improve efficiency saving money and time
3. To **reduce administrative costs** by facilitating information sharing across different registries and databases, without compromising on privacy and security
4. To **improve targeting of social programs** by using UID to identify those in need
5. To create a foundation for further **E-Government** initiatives
6. To facilitate service delivery in times of social distancing and disasters, including **government-to-people payments**

Private sector benefits

1. To **reduce administration and transaction costs to businesses** in delivering services
2. To **reduce theft and fraud** due to deficient onboarding and customer verification procedures
3. To **reduce compliance costs** in particular for industries offering financial, payments, mobile technology and health care services
4. To **reduce the liability costs of holding, maintaining and securing clients' personal data** for identification
5. To reduce time, money and effort in business **interactions with Government**
6. To contributing to growth that benefits the broader economy with a **"business friendly" environment** for companies
7. To create a foundation for the **digital economy** and better delivery of e-commerce

IMPLEMENTATION PRINCIPLES

Implementation will adhere to the following six guidelines.

CLARITY OF DIGITAL IDENTITY

Unique, complete and accurate digital identities will be established, verified, and certified

DATA PROTECTION & GOOD GOVERNANCE

The privacy of citizens and residents will be respected, and security of information maintained in line with worlds best practice. Independent oversight and addressing of grievances will be ensured.

DECENTRALIZED & FEDERATED

Existing registries and databases will not be changed. Their design will be respected. They will add and incorporate UIN as a single separate field. This will minimize disruption and speed implementation

COUNTRY OWNED TECHNOLOGY

We will rely on open standards, and open-source software or solutions relying on our own software engineers to reduce costs and promote sustainability. Vender lock-in will be avoided

INTEROPERABILITY

Open systems, open application programming interfaces (APIs) and open data standards will ensure the efficient, safe and secure exchange of information across platforms, within and external to Government

INCLUSION

The system will be designed to be accessible for registration and for usage (authentication capabilities) to ensure every person has the right to identity. This will be possible with or without local internet access

CREATING THIS STRATEGIC PLAN

This plan was developed over an 18-month period beginning on the 18th of June 2019. Prior to this, with support of the UNDP and UNICEF, experts from Estonia[5] analyzed the current situation, confirmed the benefits of a UID system, and outlined key decisions to be made. On the 19th of March 2020, a technical steering committee (Table 1) was formed to take the process forward (Government Resolution 9/2020 of 19 March).

Following the first COVID-19 state of emergency, the Committee held weekly meetings in which each Ministry presented their systems relating to identity. The Committee also learned about the design of UID systems in Cape Verde, India, and the Philippines. Based on this information, the Committee identified options and prepared a draft strategic plan in early September 2020. Presentations were made to Ministries whose technical staff participated. When a unanimous decision could not be reached by the Committee, an options paper was presented to the Council of Ministers (COM) on 27 November 2020. The COM decided to pursue Option 1, as described in this strategy.

TABLE 1: TECHNICAL STEERING COMMITTEE

TIC TIMOR (TIC)	TIC is the lead technical expert. It served as the Secretariat of the Committee and is the E-Government Agency of Timor-Leste
The Ministry of Justice (MOJ)	MOJ is a key partner. It establishes civil identity and manages civil registration (births, marriages, divorce, deaths).
Presidency of the Council of Ministers (PCM)	PCM (formerly MRLAP) coordinates Ministries and Agency participation, as part of its Public Administrative Reform Program
Ministries likely to use UIDs	Ministries of Health, Education, Finance, Interior, State Administration, Social Solidarity and Inclusion; the Civil Service Commission
UNICEF and UNDP	UNICEF and UNDP have long supported development and implementation of civil registration systems in Timor-Leste. Both have observer status

CURRENT SITUATION

Most Ministries and agencies record information and issue documents (certificates or cards) to citizens or residents, assigning in most cases a number to each person. Background data on these 20 systems can be found in Table 2 (page 5). Despite the large number of systems:

- There is no unique and definitive/authoritative identification of individuals which can be used, online and offline, across systems.
- Civil registration of vital events is currently incomplete and not fully digitalized, meaning that it cannot act as the exclusive basis for a digital identity system that is inclusive and universally accessible. The Ministry of Justice's Demographic Management Information System (DMIS) digital birth registry is outdated from a technical perspective, possibly insecure, and reliant upon a foreign vender. It lacks a legal framework and does not replace registry books, which remain the legal basis for citizenship;

[5] E-Government Agency, 2019. "Project: Development of Unique ID System for Timor-Leste Ref. No. RFP001TLS2019, Final Report."

TABLE 2: IDENTITY AND CERTIFICATE SYSTEMS THAT COULD BE LINKED TO UID

SYSTEM (ORGANIZATION)	# ACTIVE RECORDS	FEEDER DOC	INFO				BIOMETRICS			COMPUTER SYSTEM
			NAME	DOB	POB	PARENT	PHOTO	FINGER	IRIS	
1. Electronic Birth Records (Min of Justice)	400,000		◙	◙	◙	◙	◙			DMIS (computerized records only)
2. Marriage Records (Min. Justice)			◙	◙	◙	◙	◙			DMIS
3. Divorce Records (Courts)										Court Records – Divorce listed in Marriage register
4. Electronic Death Records (Min. Justice)			◙	◙	◙	◙	◙			DMIS
5. Passports (Min. Justice)	75,509	Birth certificate, BI	◙	◙		◙				PETL – Passaporte Eletroniku Timor-Leste
6. Land Registry (Ministry of Justice)										Incomplete data provided for this report
7. Billete Identidadi - BI (Min of Justice)		Birth certificate	◙	◙	◙	◙	◙	◙		One finger
8. Voter ID (STAE)	845,000	Birth certificate, Baptism certificate, declaration from Suco, BI	◙	◙	◙	◙	◙	◙		One finger
9. Health card (Min of Health)	235,137	Birth Certificate, BI; Voter ID	◙	◙	◙					Saude na Familia (SNF)
10. Driver's License (Min. Public Works)	300,000+	BI, Voter ID, Passport	◙	◙	◙	◙	◙			Terrestrial Transport Integrated Management System
11. Vehicle Registration (Min Pub. Works)	300,000+	BI, Voter ID, Passport	◙	◙	◙					Terrestrial Transport Integrated Management System
12. Student Registry (Min Education)										Incomplete data provided for this report
13. University Enrollment (various Universities)										Incomplete data provided for this report
14. Veterans Payment (Ministry for National Liberation Combatants Affairs)										Incomplete data provided for this report
15. Bolsa da Mae (Min Social Security and Inclusion)	401,698	BI, Voter ID, Passport, Declaration from Suco, Birth certificate, Baptism certificate	◙	◙	◙	◙	◙			Social Assistance Management Information System (SIGAS)
16. SAI (Min Social Security and Inclusion)										Incomplete data provided for this report
17. Social Security Payment (Inst. Soc. Sec)										Incomplete data provided for this report
18. Business registration (SERVE)	300+	BI, Voter ID	◙	◙	◙	◙				Standard Integrated Government Tax Administration (SIGTAS)
19. Tax Identifier Number (Min of Finance)										Standard Integrated Government Tax Administration (SIGTAS)
20. Personnel MIS (Civil. Service. Commission)	39,806	Birth certificate, BI, voter ID, driving license, diploma	◙	◙	◙					Sistema Integradu Jestaun Administrasaun Públika (SIGAP)

NOTE: DOB = Date of birth; POB = Place of Birth; # = number; Min = Ministry. A feeder doc is a required document needed to get another document

- Systems currently cannot readily access, match or exchange information between one another, even within limits that may be defined by Data Privacy and Protection laws;
- Data quality is an issue. This creates risk of identity fraud and duplicate records and payments. Gaps and duplications exist in most systems
- No existing systems provide digital authentication capabilities to third parties would allow those third parties to automate their processes for identification, authentication, and authorization, which means that transactions are still manual and paper-based, leading to high administrative and transaction costs.

Civil Identity

Rights to citizenship are established in the Constitution (Article 3) and regulated by Law 9/2002 of 5 November and Decree Law 1/2004 of 4 February. In principle, every birth should be registered, with registration establishing civil identity. Legally, establishing the right to Timorese citizenship is based on confirmation through his or her birth registry, that one parent is Timorese (*jus sanguine*), or that he or she was born in Timor-Leste (*jus soli*).[6] The procedures for civil registration are defined in the *Civil Code* (Law 10/2011 of September 14), the 2001 UNTAET regulation (Regulamento 3/2001) and soon on a *Civil Registry Procedural Code* present by the Ministry of Justice. The latter is currently being discussed.

However, it is estimated that only 30% (about 400,000 people) of all citizens have birth information stored in the DMIS (which is used to print birth certificates). These computerized records may be inconsistent with records in paper registries. An additional 40% (about 600,000 people) is said to have registered their birth in the paper records but there is a significant backlog in data entry from these paper registries into the electronic system. About 100,000 records can be entered each year. Without a significant registration campaign, substantial resources and an ambitious push to enter data backlogs, the civil registry will remain incomplete for some time. In addition, baptism certificates are widely used for identity purposes but these are not issued by the State. The current lack of reliable and credible identity information has, for instance, hindered Timorese who are eligible for Portuguese citizenship (i.e. those born prior to 1999) to access rights within the EU.

Furthermore, while birth and marriage registration records may help to establish identity, they are primarily used to record *events* rather than *people* and do not by themselves reliably bind with the individual claiming an identity because of the absence of biometrics, which is crucial for transactions that require higher levels of assurance.

Other Systems and Identity Cards

There are 3 prominent state provided identification cards[7] in use: birth certificates (discussed earlier), BI's and Voter ID Cards. There is one non-State provided document, a baptismal certificate. Voter ID Cards are issued by STAE, under the Ministry of State Administration. A voter can register without a birth certificate. There are currently 845,000 active, registered voters and STAE intends to establish biometric information. STAE has indicated that it would like to work with Unique ID to provide a unified approach and potentially combined registration processes.

- Though there are at least 20 systems that could be linked and validated through a central UID system, the technical committee was able to collect only preliminary and unverified information about 8 of these systems[8]
- In some cases, the issuing of a certificate or identity document depends on a foundational or "feeder" document as proof of identity. For example, to receive a passport, a citizen can present a birth certificate. Whereas, until recently, a Voter ID can use a baptismal certificate to register.

[6] As defined in Article 1 of the Decree Law 1/2004

[7] "Cards" serve as evidence that the person holding the card has registered or provided certain information to the State and that the State has validated that information to be true.

[8] Online surveys were sent to all relevant Ministries

OPTIONS

UID systems can possibly be implemented in several different ways. The technical committee identified four main options, as depicted adjacently.

Assessment of the available options

At a Council of Ministers (COM) meeting on the 27th of November 2020, the COM adopted "Option #1" (separate systems) instructing the Committee to finalize this strategy. A detailed analysis of the advantages and disadvantages of each option, and their implications for computerization, can be found in Annex 1.

Option 1: Separation -Birth Certificate Optional

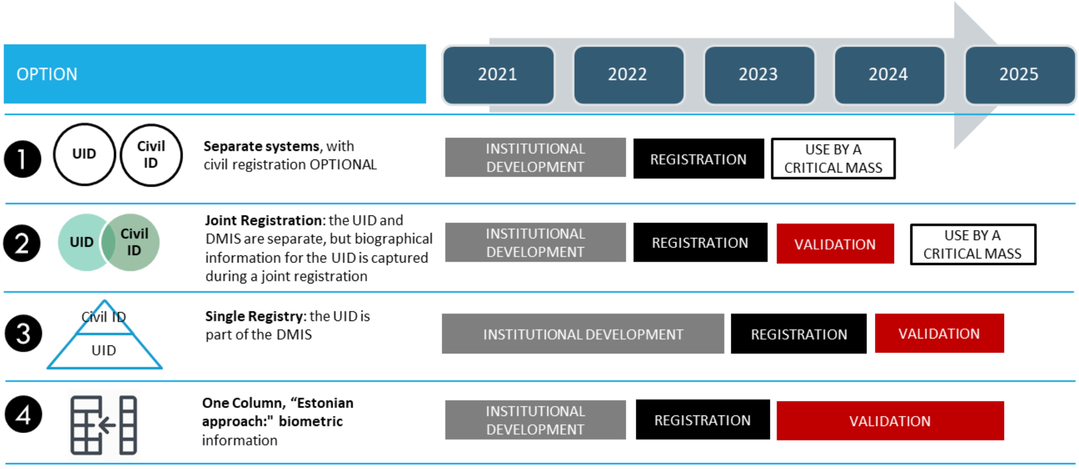
In the first option, the UID and civil registration processes are separate systems.

Civil Registration can create a Civil Identity and is the basis of citizenship. It is a high bar of identification. Timor-Leste must be sure who its citizens are. By its nature this would exclude many people from Unique ID. UID is a Digital Identity used for validation and authentication purposes, with **no bar to entry**. Everyone can receive a UID, including foreigners, orphans, refugees, stateless, and those with no existing ID. This option is inclusive to all.

A distinct legal framework would need to be established for the UID. Though separate, these have an option of linking the civil registration and the UID after initial mass registration to ensure long-term sustainability of both systems. This model is used in the Philippines, India, Pakistan, Malawi, Togo, and Tanzania; it is currently the recommended method in the Pacific and is generally considered "international best practice"[9] because it enables scale and impact to be achieved in the quickest timeframe.

The method is inclusive, fast and economical and integrates biometric information into the process. It allows registration with a birth certificate, alternative evidence or a declaration from the local authority for those without a birth certificate. An internet connection is not needed for registration. There are fewer risks, creating this separation removes dependencies on having to significantly upgrade the DMIS software, and to coordinate joint registration, which would involve significant staff and resource mobilization from the MOJ's registry directorate, as well as legal reforms that may take time. Standard UID software can be more easily adopted. It enables the "One column approach" (Option 4) by facilitating import of UIN column into existing or new data bases, but improving it by include authentication for people.

FIGURE 4: OPTIONS FOR UID SYSTEMS


OPTION
2021
2022
2023
2024
2025
1
UID
Civil ID
Separate systems, with civil registration OPTIONAL
INSTITUTIONAL DEVELOPMENT
REGISTRATION
USE BY A CRITICAL MASS
2
UID
Civil ID
Joint Registration: the UID and DMIS are separate, but biographical information for the UID is captured during a joint registration
INSTITUTIONAL DEVELOPMENT
REGISTRATION
VALIDATION
USE BY A CRITICAL MASS
3
Civil ID
UID
Single Registry: the UID is part of the DMIS
INSTITUTIONAL DEVELOPMENT
REGISTRATION
VALIDATION
4
One Column, "Estonian approach:" biometric information
INSTITUTIONAL DEVELOPMENT
REGISTRATION
VALIDATION

Civil identity administration remains within the Ministry of Justice. The MOJ can use the information in the UID system to provide improved BI Card (Smart BI). Similarly, STAE can use the UID biometrics for its Voter ID to remove duplicate and deceased voters. Ministries will still be responsible for all functional ID's, such as BI Cards,

[9] World Bank ID4D discussions. CRVS and UID should be separate ICT systems, recommended to be under the same management authority.

voter IDs, and drivers' licenses. UID will be designed to work as a platform for other systems (BI Card, Voter ID, Health IDs, Education, Social Security) so that identity is available to all.

The sole major disadvantage is that biographical data in the civil registry will need to be matched with the UID system, as ongoing registration of new births via the Civil Registration system will provide the flow of new births into the UID system. However, the UID system can and will be initially operational without this, while this linkage is created. Although the UID and Civil Registration systems are separate, a strong and well maintained Births and Deaths register is vital to ensure the UID stays accurate and up to date long into the future.

Option 2: Joint Registration – Birth Certificate Required

In the second option, the UID and DMIS are separate computerized systems, but registration is done jointly. While this method can result in consistency between digital and civil identities, and can integrate the collection of biometric information, the current, extremely low numbers of reliable and computerized civil registration records would demand three separate registration processes. The civil registry is, unfortunately, not reliable nor scalable enough to play a role in the identity proofing process.

If this method was adopted, three different processes would need to be developed. First, citizens with birth certificates (computerized civil registration) would need to be verified online (and thus a stable internet connection is required). Second, records of citizens in the paper registry (but without birth certificates) would need to have their records verified by finding their entry in a registry book; these books tend to be by year, so all original books would need to be transported to each registration site. Third, citizens who are not registered would need to complete registration afresh. A significant overhaul of the current DMIS would be a pre-requisite to this process working. The complications of this option would push back the timeline by at least one year, when compared to option #1. The requirement for a birth certificate as part of UID registration may create a barrier to registration for the UID. This option is rarely used internationally, though it was employed in Kenya.

As this option requires a birth certificate to register for Unique ID, it will exclude non-citizens and place significant barriers to the registration of orphans, elderly and others with no current ID.

Option 3: A single registry, with digital identity integrated into the Civil Registry

In this option, the UID would be a module of the DMIS with registration undertaken jointly. This strategy has been implemented in Sweden, Norway, Denmark, and Thailand, but each of these countries had decades or generations of extremely reliable and complete civil registries. No developing country has adopted this method with success recently.

Far reaching reforms to laws and systems would be required to implement this option. These reforms are likely to take years before registration can begin, pushing back the timeline significantly. A very strong initial birth registry and state capacity is required and the DMIS would need to be revamped and fully online. It will take longer to clean other data bases of duplicates, fakes and ghosts and by having one system, information will be more vulnerable to data theft due to access to and integration with multiple agencies. The additional information to be stored in the DMIS may compromise privacy.

Option 4: One column approach

This option was practiced in Estonia, as Estonia had a full set of paper birth and identity records for each citizen. The slow and steady option has also been successfully implemented by countries such as Indonesia and South Africa but this has taken several years (and sometimes decades) due to the challenges in developing a quality civil registry database or a quality paper-based population registry database. In this approach, a single UIN column is added to all databases and information is slowly validated using matching rules and algorithms across databases.[10]

[10] For example, if consistent information was found describing a citizen (name, date of birth, place of birth) in the driving license and voter registries this person would be issued a UIN

Without biometric information, duplicates will be more difficult to identify and providing authentication services will need considerably more biographical data collected on citizens.

PHASES AND PROGRAM OVERVIEW

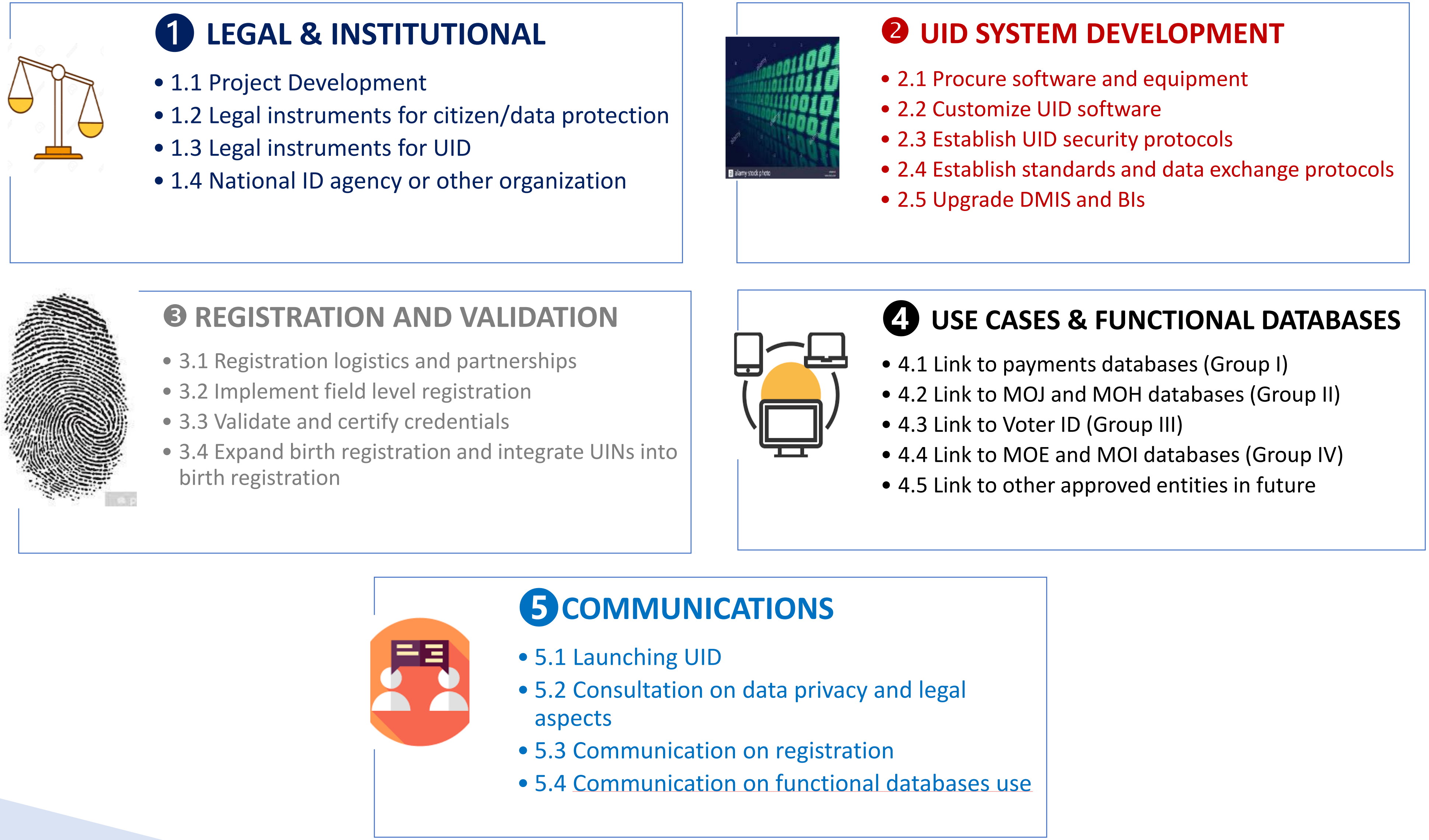
The UID project is divided into 5 phases or components as depicted below.

TABLE 3: OVERVIEW OF THE 5 PROGRAM COMPONENTS

		2021		2022		2023		2024		2025	
COMPONENT	DESCRIPTION	S1	S2	S1	S2	S1	S2	S1	S2	S1	S2
❶ **Legal and institutional Component**	This component establishes the foundations for UIDs. It develops an operational plan and feasibility study to implement this strategy. A project document will be produced by the third quarter of 2021 to raise money through the infrastructure fund, or external financing such as grants or credits. A National ID agency, institute or mission structure will be formed. A decree law on Unique IDs Systems will be approved, along with additional laws on Data Protection and Privacy, Cybercrimes and e-Commerce.	■	■	■	■						
❷ **UID Systems Development Component**	This component develops the software and processes required to organize and manage UID biographical information, biometric data and unique identification numbers, which will be linked to other databases. It procures all necessary equipment required to register and secure UIDs.		■	■	■	■					
❸ **Registration and Validation Component**	This component collects citizen and residents biographical and biometric information which will be used to establish digital identity and issue an UIN. Validation is done using biometrics to remove duplicate registrations. Cooperation with the civil registry is implemented by supporting an upgrade or overhaul of the DMIS and by implementing joint registration exercises.				■	■	■	■	■	■	■
❹ **Use Cases and Functional Databases Component**	This component makes UID registry operational with ability to carry out authentication services, online and offline, using biographic and biometric information of registered persons. It will also enable functional databases (drivers' licenses, health data, etc.) to the UID system. It cross-checks and validate the accuracy and completeness of these functional systems while providing access to services for citizens and access to information across government agencies.							■	■	■	■
❺ **Communications Component**	This component uses traditional and social media to raise awareness and build support with citizens, civil society, and Ministries to secure buy-in for the objectives of the UID system	■	■	■	■	■	■	■	■	■	■

A one-page depiction of the strategy can be found on the next page.

FIGURE 5: OVERVIEW OF THE STRATEGIC PLAN / PROJECT



1 LEGAL & INSTITUTIONAL

- 1.1 Project Development
- 1.2 Legal instruments for citizen/data protection
- 1.3 Legal instruments for UID
- 1.4 National ID agency or other organization

2 UID SYSTEM DEVELOPMENT

- 2.1 Procure software and equipment
- 2.2 Customize UID software
- 2.3 Establish UID security protocols
- 2.4 Establish standards and data exchange protocols
- 2.5 Upgrade DMIS and BIs

3 REGISTRATION AND VALIDATION

- 3.1 Registration logistics and partnerships
- 3.2 Implement field level registration
- 3.3 Validate and certify credentials
- 3.4 Expand birth registration and integrate UINs into birth registration

4 USE CASES & FUNCTIONAL DATABASES

- 4.1 Link to payments databases (Group I)
- 4.2 Link to MOJ and MOH databases (Group II)
- 4.3 Link to Voter ID (Group III)
- 4.4 Link to MOE and MOI databases (Group IV)
- 4.5 Link to other approved entities in future

5 COMMUNICATIONS

- 5.1 Launching UID
- 5.2 Consultation on data privacy and legal aspects
- 5.3 Communication on registration
- 5.4 Communication on functional databases use

RISKS AND RISK MITIGATION

Unique IDs face several key risks. The main risks are as follows:

Risk: Delays due to COVID-19

- *Mitigation:* Manage the impacts of any COVID-19 related delays as they occur. Project timelines may slip.

Risk: Data breach risking Citizen Privacy

- *Mitigation*: A Data Privacy and Protection law will be enacted to provide safeguards and accountability mechanisms for any misuse of personal data.
- *Mitigation*: By using a Privacy and Security by Design methodology, the privacy and data security of citizens is the key building block of the UID system (see Volume 2, the operational plan and budget).
- *Mitigation*: By using Open-Source Unique ID software, the base source code is visible, allowing experts, civil society, citizens and people across the world to review and improve the security of the system as time goes on.
- *Mitigation*: Significant ongoing work will secure the system, including, security reviews, vulnerability assessments, encryption of data in motion and at rest, possible tokenisation of the UIN, and automated 24/7 monitoring of all systems.

Risk: Funding causes delays in one area which affect several other areas

- *Mitigation*: A project approach of central financing will be applied. Long term access of project funds, through CAFI, grants and credits or other multi-year funding models will be pursued. Ongoing funding will be via state budget and fees collected through private enterprise use of the system.

Risk: Software development delays implementation or results in long-term dependency

- *Mitigation*; The primary approach will be to use open source software which has ongoing support, and a strong technical design and developmental roadmap. This will still require customization but removes the Vendor and Technology Lock-in risk.

Risk: Exclusion of vulnerable, disabled or marginalized people from registering

- *Mitigation*; Robust exception management provisions including allowing the Birth Certificate optional method of registration and the use of declared identities without any documentation ensures all people can register with UID. Making the registration information and any communication efforts available in local languages other than Tetum could also be a mitigation measure to reach the most vulnerable.

Risk: Resistance by Citizens, Civil Society and other institutions to UID

- *Mitigation:* With the above mitigations, and a strong communication plan with extensive consultations with stakeholders to ensure all views are heard and issues addressed

LAYOUT

Following this chapter, each component is discussed in turn. Volume II of this document provides additional details on systems design, key activities and costs.

EXPECTED RESULTS

Annex 6 provides a brief cost benefit analysis of the UID project. It demonstrates that the project will provide enormous benefits to Timor-Leste. Under a conservative baseline estimate, the UID project has an internal rate of return of 21% when using a 10-year time horizon and 24% when using a 15-year time horizon. Using a 5% discount rate over the first 10 years of the project the project will deliver benefits of $US 6.3 Million on a net present value (NPV) basis. Over a 15-year period, the NPV increases to $US 12.9 Million. Results are still very favorable under low scenario estimates.

Detailed results can be found under each component. Some key results are summarized below. Results reflect our objectives (access to services, reduced identity fraud, and costs savings), the use of the UID system and its functional databases as well as the implementation of key steps in our plan.

TABLE 4: KEY RESULTS

RESULT/INDICATOR	2021	2022	2023	2024	2025
USE OF THE SYSTEM/COVERAGE					
1. Cumulative number of people registered (issued their UIN)	---	100,000	400,000	800,000	1,000,000
2. Cumulative number of databases, services or systems that have UINs to identity and verify their clients			9	12	15
3. Cumulative records in functional databases associated with the persons UIN			547,503	1,441,931	3,188,376
GOVERNMENT RESULTS					
4. Number of duplicate or false identities discovered as a % of records			2%	2%	2%
5. Cumulative cost savings from fraud[11] mitigation due to incorporating UIN into registries ($US 100/per duplicate)			$715,962	$1,409,812	$2,470,319
CITIZEN RESULTS					
6. Estimated value of time saved (cumulative, assuming 3 hour per document and $0.74/hour)			$547,503	$ 1,441,931	$3,188,376
SERVICE PROVIDER RESULTS					
7. Estimated value of cost savings for service providers undertaking identity checks			$357,981	$1,062,887	$2,298,047
KEY MILESTONES					
8. Draft and approve a Unique ID decree law	DONE				
9. Approve the Data Privacy and Protection Law	DONE				
10. Operationalize a national ID agency, body or directorate		DONE			
11. UID open-source software system selected, customized, tested and ready for operation		DONE			
12. Upgraded, open-source civil registry database in place		DONE			
13. Certification process for outsourced registration designed		DONE			
14. Registration process piloted		DONE			

NOTE: For indicators 4-7 see Annex 6

[11] Some fraud will be saved by the private sector as well.

COMPONENT 1: LEGAL AND INSTITUTIONAL FOUNDATIONS

INTRODUCTION

Legal foundations for a UID system will be created in the early stages of the project, with most of the work completed in 2021. Strategies cover the legal and regulatory frameworks surrounding digital identity and establishing effective data and security protections for citizens. To implement this strategy, a temporary mission structure will be established to synchronize investments and **preparatory** activities. Over time, this body will be converted into an agency or organization responsible for digital identity management, which will be reflected in the legal framework. Legal changes affecting functional databases are further described in Component #4. The goals of this component and its key outputs are as follows:

GOALS

- **Establish and strengthen the legal and institutional framework required to smoothly implement the UID system**

OUTPUTS

1.1	• Develop, finance, and complete procurement for a UID project
1.2	• Create laws to protect citizens' data and privacy.
1.3	• Strengthen the legal environment surrounding digital identity (UID)
1.4	• Establish a National ID agency or other organization to implement the UID System

1.1 DEVELOP, FINANCE, AND COMPLETE PROCUREMENT FOR A UID PROJECT

In conjunction with the development and approval of this Strategic Plan, the Government is creating an operational plan and budget. These will be submitted to CAFI (the Council for Administration of the Infrastructure Fund) during the third quarter of 2021.[12] It is assumed project approval will be completed by the end of 2021. **A project approach is being taken to coordinate actions and to centralize and secure long term UID funding.**

To assist with the development of the project and the procurement of its equipment and software, technical assistance has been accessed via the World Bank. Managing the UID as a project is a transitional mechanism:

- By 2025 the mission structure will be taken over by a National ID Agency or Directorate (output #1.4).

[12] The Infrastructure Fund was established in 2011 to finance multi-year capital investment projects. Projects exceeding US$ 5 million require approval of the Council of Ministers and the Audit Court. CAFI is responsible for the Fund's operations. Standards and procedures related to infrastructure require submission of project proposals, appraisal, economic evaluation, and feasibility study, as well as the other financial procedures in the *Infrastructure Fund Administration Manual*. Key institutions involved in the process include the National Development Agency, Ministry of Planning and Strategic Investment, and the National Procurement Commission.

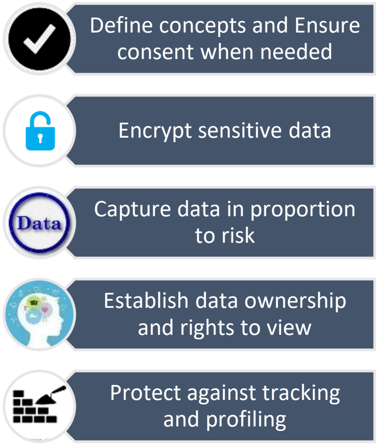
- In the meantime, the Technical Committee will function as the project board. It will supervise the mission structure management team, to be created by a decree, under article 34, Decree Law 30 2020, of 29 July. The Committee will ensure the project adopts a transparent and participatory approach when making decisions about the Unique ID system, with consensus decision-making, receptiveness to constructive inputs, and engagement with diverse voices

1.2 CREATE LAWS TO PROTECT CITIZENS' DATA AND PRIVACY

According to Article 38 of the Constitution (Protection of Personal Data)

1. *Every citizen has the right to access personal data stored in a computer system or entered into mechanical or manual records regarding him or her, and he or she shall have the right to demand the purpose of such data.*
2. *The law shall determine the concept of personal data, as well as the conditions applicable to the processing thereof*
3. *The processing of personal data on private life, political and philosophical convictions, religious faith, party or trade union membership and ethnical origin, without the consent of the interested person, is prohibited.*

FIGURE 6: EXPECTED PRINCIPLES ON DATA PRIVACY



Define concepts and Ensure consent when needed

Encrypt sensitive data

Capture data in proportion to risk

Establish data ownership and rights to view

Protect against tracking and profiling

To better specify these rights, it is essential to approve a *Data Privacy and Protection Law* and to establish its implementation and supervisory mechanisms. Work on drafting this law has commenced and it is expected to be completed by mid-2021. Expected principles are depicted adjacently. To support this, *Cyber Security*, *Cybercrimes*, and *E-Commerce* laws will also be developed and approved.

1.3 STRENGTHEN THE LEGAL ENVIRONMENT SURROUNDING UNIQUE ID

A decree law (DL) for creating the UID system, reflecting this strategy and the project document and anchored in the above-mentioned Data Privacy and Protection Law, will be required in 2021. This DL will also identify databases and registries that require change, in cases where they are regulated through decree law or Ministerial diploma. The use of UID in physical or digital format as an officially valid evidence of identity for government and other transactions, including as KYC for financial transactions (banking, insurance, money remittances) will necessitate appropriate provisioning in the applicable rules. Any effective and long-lasting identity system puts the individual's rights and needs at the center of the overall system and processes. In particular, privacy and security by design principles, and robust enforcement mechanisms will be incorporated not only in the technical system but in the rules governing every agency involved. The UID system decree law will be carefully researched and actively debated, including consultation with civil society. It will cover, amongst others:

- Robust data protection frameworks, including rules for limited data collection
- Restrictions on access by Security Services/Police to data without Court orders.
- User control over data and notice requirements
- Inclusiveness, including user choice on whether to enroll or use Unique ID
- Effective grievance redress mechanisms
- The use of outsourcing and certification in registration
- Institutional arrangements

1.4 ESTABLISH A UID MISSION STRUCTURE

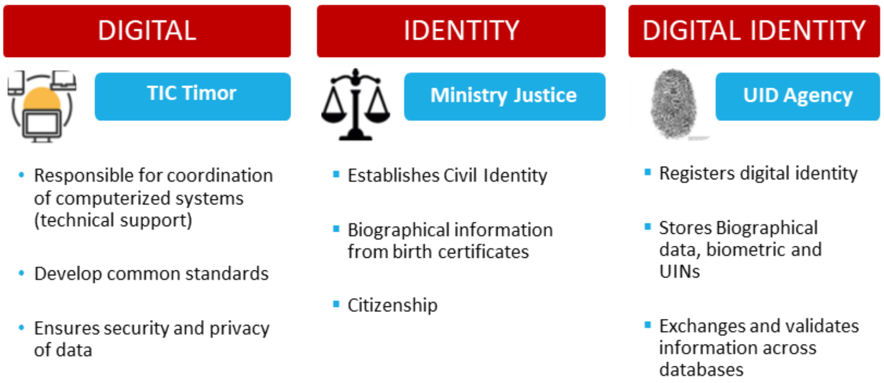
On a temporary basis, a mission structure will be created. Its formation is regulated by Decree of the Government in conformity with Decree Law 30/2020 of 29th July. The mission structure will be created immediately after the approval of this Strategy but prior to the submission of the Decree Law on the creation of Unique ID system.

A Unique ID agency can be created prior to the expiry of the mission structure in 2025, for the ongoing operation of the Unique ID system.

Most countries implement their UID programs through a semi-independent agency.[13] The advantages of this form of indirect administration include:

- The agency produces clear outputs, so can be delegated accountability to do so, in a "hands off, eyes on" relationship to a Minister or Ministers who supervise the agency
- As an agency, it can more easily contract to procure goods and services and recruit staff; this will be essential as IT services require flexible and out of the box contracting and many staff will need IT and other management competencies which are difficult to attract within the civil service

FIGURE 7: IDENTITY AND DIGITAL IDENTITY



DIGITAL

TIC Timor

- Responsible for coordination of computerized systems (technical support)
- Develop common standards
- Ensures security and privacy of data

IDENTITY

Ministry Justice

- Establishes Civil Identity
- Biographical information from birth certificates
- Citizenship

DIGITAL IDENTITY

UID Agency

- Registers digital identity
- Stores Biographical data, biometric and UINs
- Exchanges and validates information across databases

- It will be established with a culture of service delivery for other agencies and the private sector as its primary outcome, rather than building a system for its own mandate as a priority and then providing services to others as secondary. Likewise, an agency independent of sectoral functions of government is less likely be involved in questions around duplicating or entering the mandate of other agencies.

RESULTS

Expected results for Component #1 are as follows.

TABLE 5: COMPONENT #1 EXPECTED RESULT

1. RESULTS	2021	2022
1.1. Create a unique ID project		
1.1.1. Complete the UID operational plan	Q2	
1.1.2. Draft a project document and submit to CAFI	Q2	
1.1.3. Project becomes operational	Q4	
1.2. Create Laws to Protect Citizens' Data and Privacy		
1.2.1. Complete the drafting of a *Data Privacy and Protection Law*	Q2	
1.2.2. Approve the *Data Privacy and Protection Law*	Q4	
1.2.3. Draft a *Cyber Crime and E-Commerce Law*	Q4	
1.2.4. Approve a *Cyber Crime and E-Commerce Law*		Q2

[13] The "board" of the UID agency can consist of a single or multiple Ministers, for example the PM, Minister of Justice, etc.

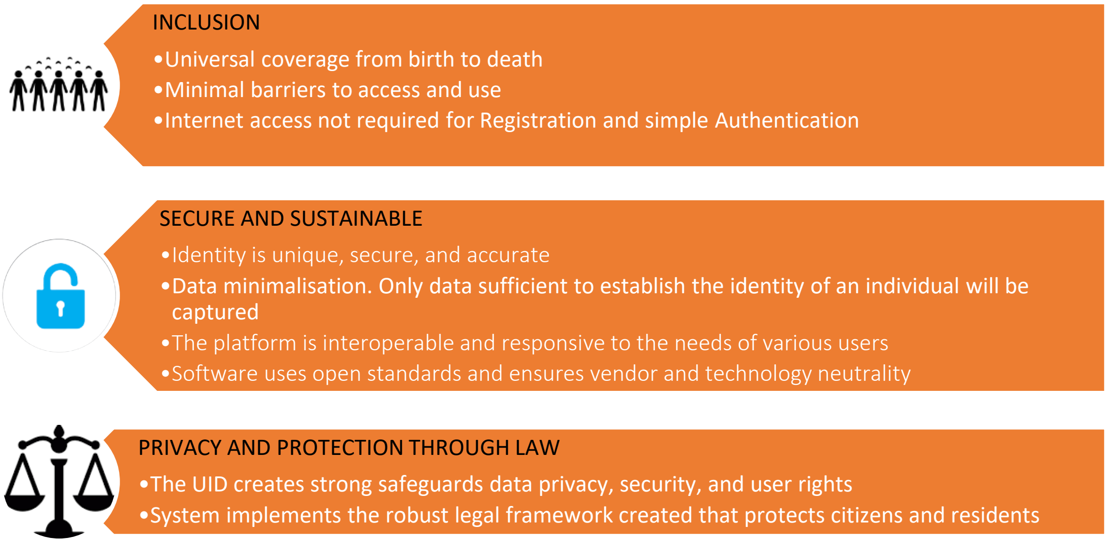
1. **RESULTS**	**2021**	**2022**
1.2.5. Develop a Cyber Security *Policy*		Q2
1.3. Strengthen the legal environment surrounding legal identity		
1.3.1. Draft and approve a Unique ID decree law	Q3	
1.4. Establish a UID Mission Structure		
1.4.1. Create a mission structure	Q3	

COMPONENT 2: UID SYSTEM DEVELOPMENT

INTRODUCTION

The UID system will be the Government's central computerized registry of digital identity information. The system, and its software, will be designed to be inclusive, secure, and sustainable. Its design will implement this strategy as well as a series of legal protections and safeguards. Design principles[14] of the UID system are as follows:

FIGURE 8: DESIGN PRINCIPLES OF THE UID SYSTEM



INCLUSION

- Universal coverage from birth to death
- Minimal barriers to access and use
- Internet access not required for Registration and simple Authentication

SECURE AND SUSTAINABLE

- Identity is unique, secure, and accurate
- Data minimalisation. Only data sufficient to establish the identity of an individual will be captured
- The platform is interoperable and responsive to the needs of various users
- Software uses open standards and ensures vendor and technology neutrality

PRIVACY AND PROTECTION THROUGH LAW

- The UID creates strong safeguards data privacy, security, and user rights
- System implements the robust legal framework created that protects citizens and residents

Component overview

The goals of this component and its key outputs are as follows:

GOALS

- **Establish a well-functioning UID technology infrastructure that can record, link, secure, and validate digital identity information, including biographical information, biometric data, and a unique identification number**

OUTPUTS

2.1	• Procure software, hardware and UID equipment
2.2	• Customize and operationalize the UID software
2.3	• Establish sound UID security protocols
2.4	• Creates software standards and data exchange protocols
2.5	•Upgrade the DMIS and Smart BI Systems

[14] Adapted from the Principles on ID for Sustainable Development at https://id4d.worldbank.org/principles

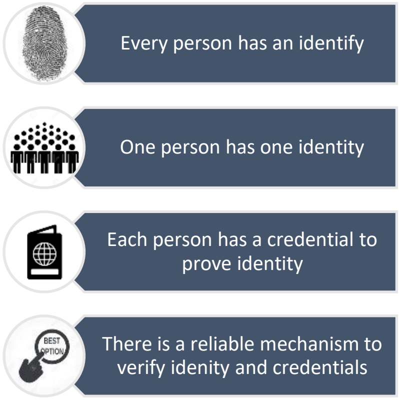
2.1 PROCURE SOFTWARE AND EQUIPMENT

A wide range of hardware, software and equipment are needed to implement the UID project. **During the first half of 2021, a detailed procurement plan and budget will be developed.** It is expected that the project will procure, amongst others: server infrastructure, laptops, printers, biometric capture and authentication equipment (fingerprint scanners, iris scanners, signature pads, cameras), verification tools, as well as a wide range of security and software applications. Technical assistance will be arranged to assist TIC Timor to develop specifications for equipment and software.

The software procured will adhere to the principles outlined above in Figure 8. In particular, it will ensure open standards and vendor and technological neutrality. This will allow Timor-Leste to own the system fully, with the ability to change and customize components and vendors as need arises. The Government will control all source code and store all data securely within its borders. No data will leave Timor-Leste. The Government will not develop UID software from the ground up, but will utilize existing free open-source solutions and customize to its requirements with assistance from systems integrators as needed.

TIC Timor and the KTE will undertake an exhaustive search, completing a comparative analysis of available software. Once selected, the team will commission a system integrator to assist TIC to develop the open-source software, ensuring it meets all privacy and security needs and can undertake the functions outlined in this strategy. A benefit of using open-source software is that it may develop in new directions and can continually evolve to meet new challenges. Competition will be encouraged, bringing down costs and avoiding lock-in to a particular proprietary technology or vendor. As it is open-source, any vendor may bid to provide support as the systems integrator.

FIGURE 9: BUILDING BLOCKS OF ID SYSTEMS


Every person has an identify
One person has one identity
Each person has a credential to prove identity
BEST OPTION
There is a reliable mechanism to verify idenity and credentials

Similarly, the planning and provisioning for a primary and disaster recovery datacenter will be made to meet international standards, which is a datacenter with zero single points of failure and redundancies for every process and a data protection regime with 99.9% uptime

2.2 CUSTOMIZE AND OPERATIONALIZE UID SOFTWARE

A digital ID uniquely identifies a person and provides that person a means to prove identity to a third party when transacting online. The basic building blocks of this system is that every person has a one identity, and that this identity can be proved or verified (Figure 9). As such, the UID registry will need to be highly protected, frequently backed up, and managed as the definitive source of all governmentally warranted identity and authentication. As the tip of an identity and authentication pyramid, identity data will be cascaded and reflected into each linked, lower-tier information system. UID registry isn't authoritative on personal information like citizenship, or authorization and rights such as to vote or drive, that remains with the functional IDs in the relevant ministries.

Functionality

The system is expected have the following main functions:

FIGURE 10: KEY FUNCTIONALITY OF THE UID SYSTEM

FUNCTIONS

- Internet Access will not be required for registration and simple authentication.
- UID data will be stored separately from other key identity information, such as birth certificate numbers;

FUNCTIONS

- The UID will store minimal biographical information including a person's name, date of birth, place of birth, and potentially, the names of parents for those under 13 years old (not required for children with no known parent(s));
- The UID will store biometric information—a facial image and fingerprints, perhaps iris data; biometric information will be collected for all persons after reaching a certain age (presumed to be 13)
- The UID will be the preferred definitive source of biometric information to be used across government; this will eliminate duplication of costs, information, and efforts;
- The UID will generate, automatically, a UIN. The UIN will be a set of random numbers (with 2 control digits) and will not contain attributes of the person. The UIN is expected to be 10 digits[15]; however, the UIN may be tokenized to improve security of the system;[16].
- The UIN by itself will not be used as an authenticator or password to access services;
- The UID system will cover all people residing in Timor-Leste, including Citizens, Residents, Refugees, and others.
- The UID will encourage universal coverage, especially for people in difficult-to-access areas through both online and offline facilities, eliminating the need for internet in rural areas;
- UID data will assist the MOJ so that MOJ can generate and print a Smart BI Card at its own discretion;
- UID data will assist STAE so that STAE can generate and print a Smart Voter Card at its own discretion;
- The system will be able to function as an authentication provider in areas of no internet and to employ offline mechanisms of authentication through, for example, a physical identity card with biographic information and a photograph and a QR code, or a Smart BI Card;
- The system will provide robust exception management protocols to enroll/register as well as authenticate individuals with the objective of eliminating exclusions and hardships to citizens/residents.
- The UID system will facilitate validation and accuracy of digital identity data across all functional databases;
- The UID system will ensure the efficient querying and linking of information across all functional databases, subject to the UID and Data Privacy and Protection laws;
- The UID system will protect the privacy and security of citizens and residents in everything it does; the UID system will adhere to a secure set of data exchange and access protocols that protect privacy across functional databases
- A minimal set of metadata about the registration process will be stored, to facilitate offline data capture

System architecture

There are two main possibilities for choosing the UID system software. Closed-Source and Open-Source. Each has its advantages and disadvantages, but as has been seen with other core Government IT systems, costs can climb significantly with some closed-source systems. Using open-source software and utilising open standards increases interoperability of the software across many government and private systems, significantly reducing the costs of integration. This also avoids the vendor lock-in that has occurred elsewhere within government, as the government has complete control of the software.

A full search and select for the most appropriate software will need to be carried out to ensure that the best solution is implemented. However, the easiest solution for the software development is to customize an existing, open-source, well-tested system such as MOSIP (Modular Open Source Identity Platform, https://www.mosip.io/)[17] or similar alternatives.

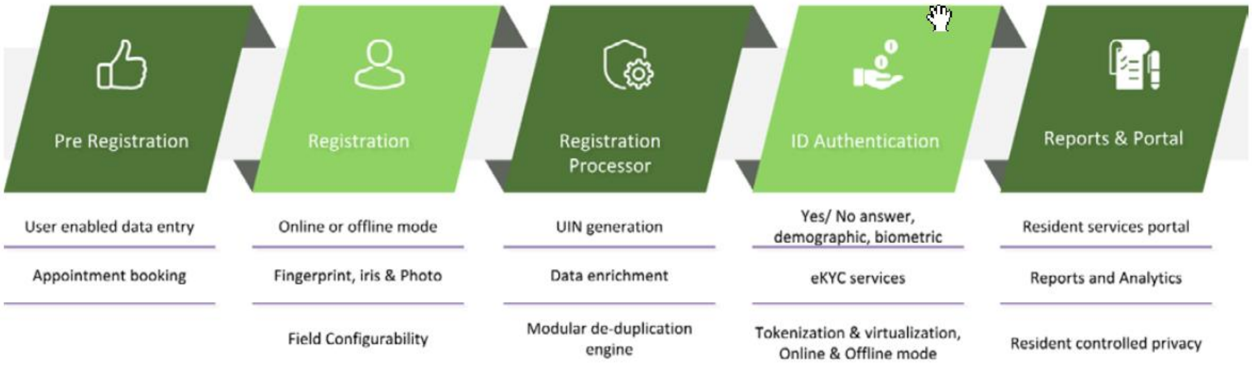
[15] The World Bank (2018) documents UINs in 70 countries. It finds: (i) in 90% of all cases the length of the personal identifiers was between 9 and 13 digits; with a few exceptions, they consisted entirely of numerals; (ii) almost without exception, part of the UIN is a unique serial number, which is constructed in three different ways; two are random and one is sequential. Control digits are numbers computed from, and then added to, the randomly generated stem via a checksum or hashing function. They are used to check data entry errors such mistyped digits, transpositions, etc.

[16] The World Bank suggests using tokenization to improve system security. https://id4d.worldbank.org/guide/tokenization

[17] MOSIP is an open-source software for building identity systems. Designed in India, it is currently being either used or pursued in Morocco, the Philippines, Togo, Ethiopia and Guinea.

Key elements of the basic architecture are that the system has independent and interchangeable modules with API-based implementation, effectively using service-oriented and micro-services approaches. It is possible to customize each of these modules at a component or feature level to suit the Timor-Leste context. This also enables an implementation to integrate with existing databases easily. Key modules expected in the solution include, at a minimum: (i) Pre-Registration; (ii) Registration; (iii) a Registration Processor; (iv) ID Authentication; and (v) Reports and Portal Access

FIGURE 11: KEY MODULES



It is also key that the UID system functions effectively and is trusted by the population. This is done by ensuring that the UID system provides:

Privacy

Security and Privacy are first and foremost in the design. It must be designed with these tenets from the outset and these capabilities are not added as an afterthought. User privacy should have a consent framework that lets the user choose what to share and when. It must be transparent and lets the user know what they have shared and when, and also allows the user to lock authentication features that they wish to restrict.

Security

From a security perspective, all personally identifiable information is encrypted and inaccessible to internal and external parties without user consent. All flow of such information is in trusted environments only. The trust is established through PKI, license keys, policies and infrastructure security.

Scalability and manageability

Two critical factors when it comes to scalability are first, that the platform should work at country population scale, and second that it must provide continuity as technology evolves. It must be designed with easy auditing, monitoring, testing and upgrades in mind.

UID Cards

There are many options concerning the nature of the UID card, which can be used as a credential to verify the user's successful registration. The principle will be to keep it simple and cost-efficient, adopting 2D barcodes (QR codes) which will be sufficient for fingerprint and cryptographic signatures and can digitally authenticate the holder online against a server via internet or mobile services. The cost of generating a QR coded card, depending on the material used, is about $US 1 per card.

2.3 ESTABLISH UID SECURITY AND PRIVACY PROTOCOLS

To have confidence in online services, users will demand identity information to be accessed only by those who have legitimate authority and purpose. To ensure security, a wide range of risks must be managed, including hacking, identity theft, phishing, and other unauthorized uses. **Security of the UID system is paramount.** To address security:

- All personally identifiable information will be encrypted;
- There will be an ability to quarantine and isolate when attacked or compromised;
- Response plans will be written and tested to respond to security attacks and threats;
- There will be clear and transparent restrictions on access to databases;
- Security will be built into all systems;
- Access to an individual's data will be based on the person's consent;
- Individuals have the right to access and correct their data
- The system will allow for secure offline authentication;
- All events will be auditable and non-repudiable (cannot be reversed);
- Records can never be deleted;
- Vulnerability assessments will be routinely performed;
- There will be 24/7 automated security monitoring of all systems;
- There will be tamperproof logs enabling oversight of how these data are being used

2.4 STANDARDS AND DATA EXCHANGE PROTOCOLS

As the E-Government Agency of the Government, TIC-Timor will ensure different electronic systems can exchange data in a smooth and efficient manner.

Adoption of ISO Standards will establish specifications and procedures in terms of the operation, maintenance, and reliability of materials, products, methods, and services. They will regulate the capture, storage, transmission, and use of identity data, as well as the format and features of identity credentials and authentication protocols. As described earlier, an emphasis will be placed on open-source software and vendor neutrality. Amongst others, standards will be developed in terms of:

- Security and encryption
- Registration and registration agents, including their training requirements and certification
- Registration hardware which can be used
- Software in use in functional databases that will be linked to the UID
- Access to UID data, for institutions and individuals

2.5 DMIS ENHANCEMENT AND BI CARDS

Although the UID system and the DMIS (Demographic Management Information System) are separate systems and although the project does not depend on the DMIS, **the unique ID system would greatly benefit from the adoption of new, open-source civil registry software** and an expansion in the number of citizens with birth certificates, for the ongoing sustainability of UID. The UID system will also depend on data on birth for the registration of children to create a UID record and deaths to deactivate a UID record.

FIGURE 12: DMIS SOFTWARE CONSTRAINTS

- The data is incomplete as there is a significant backlog of paper records to be entered (approximately 600,000);
- Electronic data may not match paper registry records which legally confer civil identity
- Security and privacy safeguards are insufficient for a UID system to rely upon;
- The data entered is likely to have duplicates and errors (such as spelling mistakes);
- The DMIS uses Oracle 11G software. This was last updated 4 years ago, is now out of date and is no longer mainstream supported. This creates significant risks for security, support, and integration into other systems;
- The different modules of the DMIS cannot be easily or reliably linked
- The software is managed by an external vender, through a service contract funded through the state budget, at significant cost. This arrangement is expensive and inflexible;

This project proposes a new CRVS system to be implemented by the Ministry of Justice, using open-source, open-standard CRVS software that has modern and more convenient methods for registration of births and deaths.

The budget for this improved CRVS system is included in the UID project, but will be managed by the Ministry of Justice, working with the UID Mission Structure to ensure compatibility and interoperability in the systems, reducing waste and duplicate efforts.

Similarly, with the STAE Voter ID registrations, UID will improve the overall numbers and accuracy of the Births and Deaths registers by ensuring that all people born and dying in Timor-Leste are recorded in the government systems.

Civil registration and vital statistics (CRVS) software

Robust, electronic CRVS software can better track and monitor life events and can lead to potential cost savings. The current DMIS records civil registration data, including births, marriage, divorce and deaths. It has 8 modules, with each module using different identifying numbers. While these numbers are unique at any point in time, they record attributes of the citizen, and therefore change depending on circumstances (for example, when place of residence changes).[18] As depicted adjacently, the existing DMIS faces several important problems.

To solve these problems, and to ensure the DMIS can be more effectively linked to the UID software, **the DMIS ultimately requires new electronic CRVS (Civil Registration and Vital Statistics) system, based on open source and open standards,** such as OpenCRVS (https://www.opencrvs.org).[19] Therefore, the Government will:

1. Investigate the feasibility of adopting and customizing open source, modern, web-enabled CRVS software
2. Finance the upgrade, rollout and support of this CRVS software

BI Cards

Once a UIN is assigned, the UID system can be used by the Ministry of Justice to print "SMART" BI cards; a module, with access rights for the MOJ will be developed to implement this. These will replace (upgrade) existing BIs.

It is necessary to complete a detailed cost-benefit analysis on the type of card to be employed. Smartcards with an integrated chip can cost between $1 to $50 each, depending on the material, volume and specifications. Several options will be considered, including:

A smart card (with an integrated chip). This has tended to be used in advanced economies where a private key digital certificate in the card that can be used with a home reader, enabling people to plug the reader into their PC and verify their identity online. However, even those countries are now transitioning to mobile IDs (using a smartphone application and/or digital certificate in the personal SIM card). According to the World Bank, many countries that have implemented multi-purpose smartcards (e.g. Thailand, Malaysia, Tanzania) have struggled to realize those multiple purposes. Indonesia has implemented single-purpose smartcards for which the chip has had limited usage.

Printing encoded data into a bar/QR code, e.g. digitally signed demographic data. This can be used in offline contexts and universally. Other authentications, including in a deferred batch mode, can be carried out later against the central database, assuming the availability of at least a 3G internet connection.

[18] The birth certificate ID number, for example, has 20 digits, while the ID recorded in the DMIS consists of 17 digits, including a local municipal code, DOB, and control digits.

[19] The World Bank Blog: https://blogs.worldbank.org/health/ building-national-civil-registration-systems-ensure-effective-service-delivery which also identifies: These include WCC (HERA), Canadian Bank Note (National Identification & Registry), DelaRue (DLR Identify™ for CRVS), Digitech (Civil Status solution), KP VTI (Civil Registry Systems), Axiell Group (vital records and statistics SOFTWARE), Genesis (WebLE), Promadis (Births, Deaths and Marriages Registry), and Object Consulting (CRVSNOW). CRVSNOW is available free to low-income countries to help modernize their CRVS systems.

By closely integrating the UID System and the new CRVS system, the expectation is that the UID cards created in this project will be able to be replaced over time for Citizens with the "Smart" BI card. Non-Citizens or those who cannot prove citizenship will continue to use the UID Card, as BI cards are solely for Citizens of Timor-Leste.

RESULTS

This component establishes a working, computerized UID system that is secure and accurate. Expected results are:

TABLE 6: COMPONENT #2 EXPECTED RESULTS

ITEM	2021	2022	2023	2024	2025
KEY RESULTS					
UID software system selected, customized, tested and ready for operation		By Q3			
INTERMEDIATE MILESTONES					
Equipment and software procurement plan completed	By Q2				
Assessment of possible UID software completed	By Q3				
Service contract for UID software support signed	By Q3				
Feasibility of CRVS open source software completed		By Q1			
Upgraded CRVS in place (if feasible)		By Q3			
Data exchange and software protocols in place			By Q1		

COMPONENT 3: UID REGISTRATION & VALIDATION

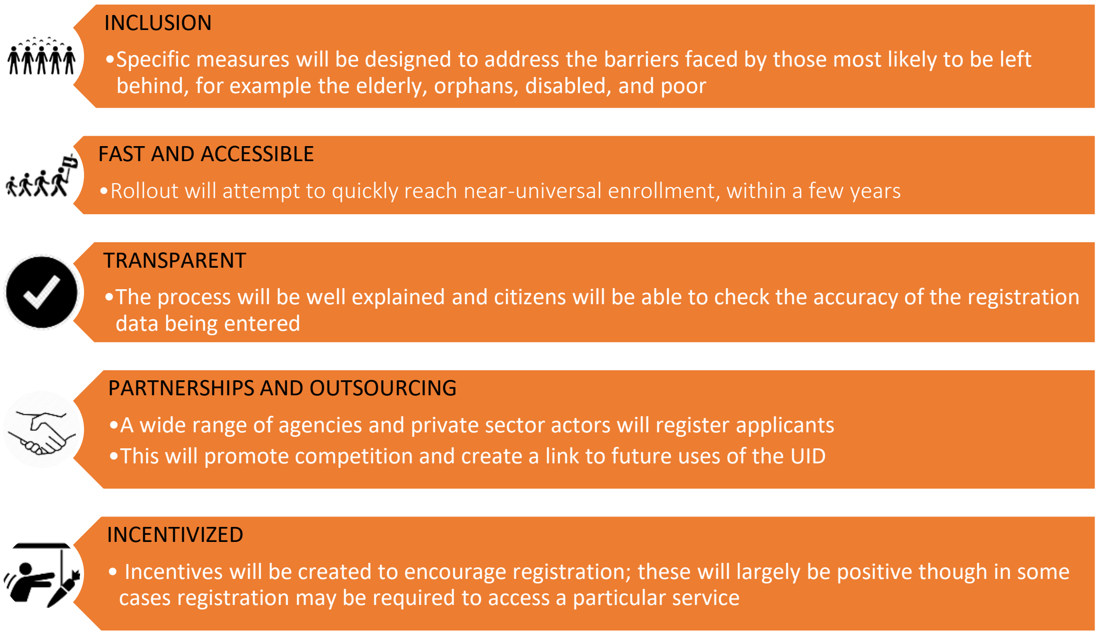
INTRODUCTION

To be successful, the UID system will need to quickly achieve a critical mass of users. In the beginning, large-scale registration campaigns will be necessary. This will make identification accessible to substantial segments of the population, within a short timeframe. The campaign will include communications as well as concerted outreach, including visits to all rural Sucos. A detailed plan, coordinated with multiple actors will be developed during 2021.

Registration collects the data required to establish and verify digital identities; it also provides credentials (a simple card) to those successfully completing the process. The registration process will avoid: (i) long distances to the nearest registration point; (ii) high direct and indirect costs of obtaining a UID; (iii) cumbersome enrollment processes and requirements. Addressing these issues will encourage maximum participation.

A large-scale registration campaign, on its own, is not however sufficient to sustain UIDs. In order for the database to remain accurate and useful, registration campaigns need to be complemented and followed up by continuous enrollment (of new people, especially children through the birth certification process) as well as the updating of records of people who have already enrolled. People may change their name or other key information. This is referred to as a "**stock and flow**" model, the stock being the existing database of identified individuals, and the flow being the continuously added new individuals. Without continuous updating, records will slowly become out-of-date, leading to repeated and costly data collection exercises. The principles underlying registration are:

FIGURE 13: PRINCIPLES OF UID REGISTRATION



INCLUSION
- Specific measures will be designed to address the barriers faced by those most likely to be left behind, for example the elderly, orphans, disabled, and poor

FAST AND ACCESSIBLE
- Rollout will attempt to quickly reach near-universal enrollment, within a few years

TRANSPARENT
- The process will be well explained and citizens will be able to check the accuracy of the registration data being entered

PARTNERSHIPS AND OUTSOURCING
- A wide range of agencies and private sector actors will register applicants
- This will promote competition and create a link to future uses of the UID

INCENTIVIZED
- Incentives will be created to encourage registration; these will largely be positive though in some cases registration may be required to access a particular service

Component overview

The goals of this component and its key outputs are as follows:

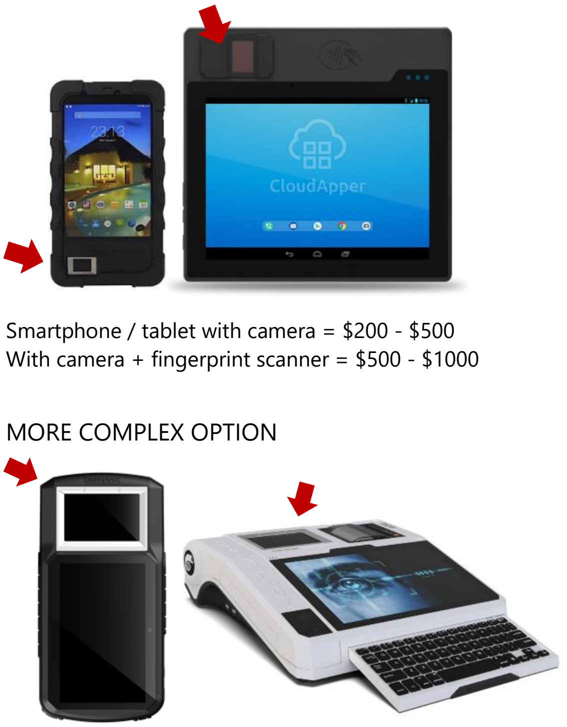
GOALS		OUTPUTS
Register and validate 1 Million UID users by end of 2025	3.1	Registration logistics and partnerships
	3.2	Implement field level registration
	3.3	Validate and certify credentials
	3.4	Expand birth registration and integrate UINs into birth registration

3.1 REGISTRATION LOGISTICS AND PARTNERSHIPS

Intensive planning will be required to implement the two main types of registration:

- Registration in rural Sucos, largely implemented centrally by the government
- Registration in urban and semi-urban areas, largely implemented by approved registration agents

FIGURE 14: TYPICAL REGISTRATION EQUIPMENT



SIMPLE OPTION

Smartphone / tablet with camera = $200 - $500
With camera + fingerprint scanner = $500 - $1000

MORE COMPLEX OPTION

Tablet with slap fingerprint (4+4+2) + iris scanners: $2,200-$3,000

Source: Internal World Bank documents

To promote registration, the Government will lead a series of communications initiatives (Component #5, describing why, how, and where to register) and will develop a detailed logistical plan.

Planning for Suco Registration

During the COVID-19 state of emergency the Government successfully distributed cash payments to roughly 300,000 households. This was a multi-agency effort, including the Ministry of Social Solidarity and Inclusion, the military, Municipalities, and banks. Distribution was at Suco level, with households meeting at a central point and observing sanitary and social distancing protocols. Disbursement took approximately 3 days per Suco and there are 452 Sucos. There are however 65 cities and towns in Timor-Leste and some 30% of all Timorese live in urban areas. In India, a single registrar on average can register 40 persons per day. For rural Sucos, the registration teams will physically visit the locations to register people.

First, the operational plan will design **any incentives to be in use**. These will consist of a mix of rewards and sanctions. The design of these incentives will be done in a way to minimize exclusion from services, respect people's rights to access basic services, and ensure that the supply of registration services can meet generated increases in demand for registration. Possibilities include:

TABLE 7: POSSIBLE REGISTRATION INCENTIVES

TYPE	POSSIBLE INCENTIVE
POSITIVE INCENTIVE (REWARD)	• Campaign to promote Financial Inclusion. Open/Register a bank account with UID and receive $5 in that account. • A service is provided on a priority basis or is provided more timely if a person has a UID • A social protection payments can be made quicker if the recipient has a UID
NEGATIVE INCENTIVE (REQUIREMENT)	• A bank account can be opened / maintained only with a UID (to deter money-laundering) • To receive a Tax ID, the entity must have a UID; to register a company, a UID is required • To receive a government service payment (e.g. veterans' benefits, government salaries, signing a government contract) a UID is encouraged by speeding up payment times • Robust exception management systems will however be made available as a rule where ever negative incentives are invoked to ensure genuine cases are not subject to undue hardship or unfair exclusion

Second, the operational plan will identify methods to **separately register particular groups**, such as the military, civil servants,[20] students, the disabled, overseas Timorese, etc. Similarly, all registration procedures will include the use of "fast lanes" (for example, for pregnant women). Different segments of the market will be treated differently.

Registration by Government agents: Rural Sucos

Each of the rural Sucos is expected to be visited by a team of 5 registry personnel for a period of 4 days (together with security and other support staff).[21] This implies the need to contract about 5 teams (25 persons) to complete coverage each year. In future years, the number of registry personnel may decrease. Contract staff will receive both a fixed salary and an incentive payment (per successful registration).

Where possible, registration will be carried out in conjunction with other Suco based initiatives including, civil registration, the census,[22] etc. STAE has indicated that it will be willing to work with UID on its Voter Registration initiatives. Combining multiple registration initiatives will greatly reduce transport, staffing and other costs by sharing resources.

Registration by approved agents: Urban and Semi-Urban Sucos

In Urban and Semi-Urban locations, a wide range of third party agents will be potentially certified to undertake registration (data collection). This is possible because all data is encrypted and the devices secured and certified, the Registration Agents will not have any access or store any identifiable data, so there is no risk of information being stolen. Agents may include private sector parties, municipal governments, banks, mobile phone providers, post-offices, hospitals, the Ministry of Justice, STAE, and others. Agents will be paid a flat fee for each successful (i.e. validated) registration record; this will incentivize the agent to find customers, for example, at offices, large high schools, etc. In India, the fee paid to the agent is $US 1 per registration, but it is likely to be more expensive in Timor-Leste. $2 per successful registration was included in the budget. Agents will be certified by the Government that:

- They are using approved and certified equipment (tablets, etc.) and software
- Their staff is trained and successfully passed an examination concerning the process
- They are a registered business or entity in good standing, with sufficient IT experience

A system and process of certifying agents will be developed. In other countries, where registration services are outsourced, agents often: (i) are quite innovative in finding customers; (ii) use promotions and communication; (iii) are possibly responsible to procure the equipment they are using, and often procure at very competitive prices. Since registration is continuous (will be done every year), agents will eventually need to operate in rural Sucos.

[20] This would be done at the office, on a particular day
[21] 25 person days would be sufficient to register 1000 persons
[22] It is unlikely the timing will match for the Census, unless the Census is further delayed.

Training

A full, certified, training program will be developed for all personnel undertaking registration. This will include customer services.

Help line

A toll free help line will be created to answer questions arising from registration (by customers or agents).

Consultation

Once the process is initially designed, a consultation process with NGOs and other stakeholders will be held to finalize the process with their feedback.

3.2 IMPLEMENT REGISTRATION OF 1 MILLION PERSONS

Prior to rollout, the registration will be piloted; this will include optimizing the sensitivity of biometric uniqueness checks. The pilot may show adjustments will be needed in the registration process. The project and procurement plans will need to be flexible enough to allow for such changes.

Registration will collect the minimal biographical information, and biometric data needed for UID registration. Any other information that may be collected such a mobile phone number, ID collection point, registration metadata and similar will also be stored securely. No costs will be paid by applicants.

The system will be implemented offline, so data will ultimately need to be uploaded to the UID server. In India, for example, postal addresses are collected in order to send UID “cards” (credentials) to successful applicants, but because of the lack of addresses in use in Timor-Leste, cards will need to be distributed differently, with Suco offices being a central ID collection point. This will be a challenge.

To be registered, people will either require other forms of ID or will need to be verified by the Suco Chief (or other witnesses). This will allow applicants to register in a way that is most convenient to them. When an applicant arrives at a registration desk, the following steps are expected to take place:

1. The applicant presents his or her ID for a ‘verified’ identity or is witnessed by a Suco or Government official for a ‘declared’ identity.
2. The registrar scans a copy of the applicant’s supporting ID information or records the witnesses name.
3. The registrar records the name, date of birth, and potentially parents’ names for children (i.e. biographical data)
4. The registrar records basic contact information, including mobile phone and the pickup location for the UID “card” (credential), if not issued immediately.
5. Metadata describing the registration process will be captured by the system without requiring data entry (location, date and time stamp, device information, etc.)
6. The applicant checks that the data entered is correct to ensure it is accurate; typically, 2 screens will be in use, one for the data entry personnel and 1 for the applicant to observe what is happening
7. Biometric information is taken (photo, fingerprints and possibly iris print) and quality is assessed live by the software so as to ensure it meets minimum standards; this too is also checked by the applicant (for example, that the photo is acceptable)
8. The system completes automated checks to ensure the information is complete and appears valid
9. A receipt of application is provided to the applicant; depending on the technology in use this would ideally be printed by the system at this point, though paper receipts may also be employed.

Periodically, the registrar will upload the data to the UID server.

The target is to register 1 Million persons by the end of 2025, as follows.

FIGURE 15: EXPECTED CUMULATIVE NUMBER OF PERSONS REGISTERED

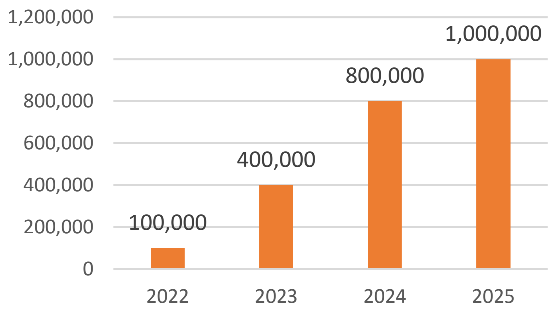
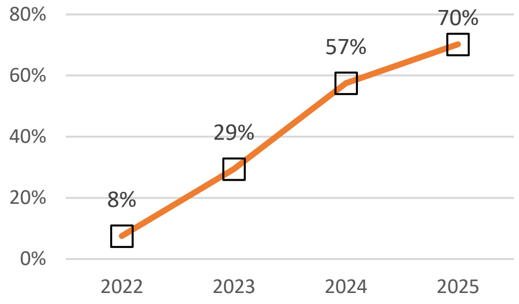


FIGURE 16: EXPECTED CUMULATIVE % OF THE POPULATION REGISTERED



3.3 VALIDATION AND CREDENTIALS

Once registration data is uploaded, the UID agency will verify its completeness and accuracy. Duplicate biometric information will be identified and addressed. Validation will also monitor registration trends, identifying outliers; this may indicate cases where registration personnel are taking shortcuts. Once the information uploaded is validated, external agents will be paid (on a per-record basis).

Successful applicants will be issued a simple card, certifying their registration, and containing a photo, biographical information and a QR code and their Unique ID number (UIN) or a tokenized UIN. Distributing these credentials back to each UID holder is expected to be a challenge and to possibly consist of:

- Issuance of an electronic UID credential through a mobile phone or email address; there are many smartphone apps available for creating digital credentials.
- Issuance of a simple plastic UID card, to be picked up at a selected location, for example the Suco office (**a pick-up point**). This will contain a photo, simple biographical information, the (possibly tokenized) UIN, and a QR code. The card will be as cheap and efficient as possible. Recipients will be provided phone calls, SMS messages, etc. reminding them to pick up their card.

Unique ID numbers or a tokenized UINs can therefore be used for authentication, as a "credential." The holder can present his or her UIN to a service provider, who then uses the ID number to look up the person's record in a database and then verify the identity by checking his or her biometric information against the record in the UID system. **The UIN is like a username while the biometric data is like a password.** Other password options like One-Time-Passwords via SMS will also be investigated for use by the UID system.

BI Cards and the Ministry of Justice

At this point, the validated information can be exchanged with the Ministry of Justice for issuing of an upgraded ("SMART") BI card and for supporting the Ministry's work in validating citizenship or civil identity. These steps will require additional information held by the Ministry of Justice.

3.4 EXPAND AND UPGRADE BIRTH REGISTRATION

One way to ensure that the UID number is used by all government and private agencies is by issuing it at birth and inserting it into the birth certificate of the infant. Since the birth certificate is the original identity document, it is likely that this number will then persist as the key identifier through the individual's life events, such as joining school, immunizations, voting, etc. Since the name will be a mandatory field in the UID database, a procedure for delayed naming of the child will need to be devised. This would ensure that the UID can be allotted at birth.

RESULTS

The registration activities described in this component are intended to reach a high level, as soon as possible. Expected results are as follows:

TABLE 8: COMPONENT #3 EXPECTED RESULTS

ITEM	2022	2023	2024	2025
KEY REGISTRATION RESULTS				
Cumulative number of people registered (having valid UID data)	100,000	400,000	800,000	1,000,000
% of the population with UIDs	8%	29%	57%	70%
INTERMEDIATE MILESTONES				
Consultation on registration held	Q2			
Registration plan and logistics completed	Q3			
Certification process for outsourced registration designed	Q3			
Training certification program designed	Q4			
Number of registration agent entities approved	2	5	10	10
Registration process piloted	Q3			
Registration begins		Q1		
New BI card developed by the MOJ, using information from the UID		Q2		
Number of newborn births registered and provided a UIN			29,472	30,150

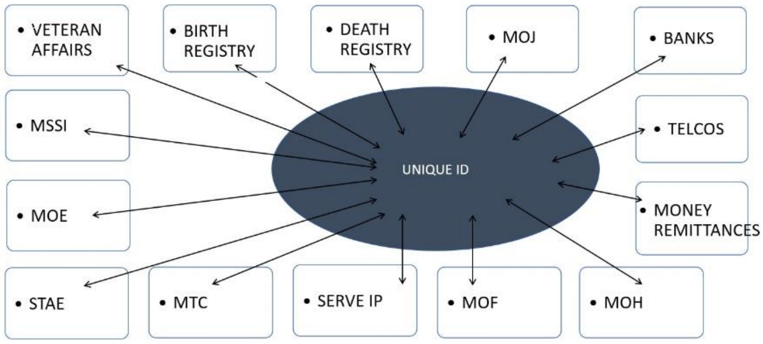
COMPONENT 4: USE CASES AND FUNCTIONAL DATABASES

INTRODUCTION

The UID system can significantly improve people's access to public and private services, as well as the efficiency and quality of these services. Potential applications of the UID can cover a wide range of sectors, including financial services; mobile and telecommunications; social protection; health and education; taxpayer identification and revenue generation; voter identification; civil servant payroll management; and civil registration. Ultimately, digital ID systems that allow people to prove their identity online stand alongside connectivity, digital payment systems, strong data governance, and digital literacy as key foundations for the transition to an inclusive and resilient digital economy and society.

The goal of the Unique ID system is to provide a safe, secure and trusted mechanism for citizens to identify themselves to service providers and for these identities to be verified – both in person and online. This will include data deduplication across multiple government systems to remove ghost, duplicate and fake identities. Data sharing will be done with citizens' privacy foremost in mind. The Unique ID system will not share information across government areas that is not necessary nor lawful for the tasks needed by that government or private entity. Generally, the Unique ID system will provide a YES/NO answer to the service provider who is trying to identify a citizen or resident. Is this the person or not? It will not provide more information than is needed to answer this question. A consent based system of sharing individual data to a trusted third party will be devised. The e-KYC of India provides a model wherein secure server to server transfer of digitally-signed and machine-readable data is provided against biometric consent of the individual, following authentication as consent of the data subject. This is known to have increased customer convenience, induced business efficiencies, reduced sharing physical documents and helped digitalization at a systemic level.

FIGURE 17: UID AS A CENTRAL REPOSITORY OF DIGITAL ID DATA



Linking to the UID system requires few changes in the functional databases maintained by government and private entities. Generally speaking, once security is ensured, these systems will simply need to add "another column" recording a UIN for each record. Each entity will require authentication equipment at customer facing areas.

The UID system will collect minimal data on the individual. The functional databases contain details on the individual, as per their mandates and its legal requirements, for example whether the person a citizen, can drive a car, or has a valid visa. Therefore, the UID system does not collect, hold or store any information new information about the individual, except their biometric information showing they are unique. The UID is a mechanism for linking and verifying data across functional databases.

While registration (component #3) aims to maximize the number of citizens and residents with UINs, this component aims to maximize the number of public and private sectors linked to the UID system, with the capability of verifying digital identities.

Component overview

The goals of this component are to:

- **Leverage the UID to authenticate individuals and link their UIN to functional databases, to improve decision making and access to services**
- **Improve the accuracy of identity information managed in functional databases**
- **Reduce identity fraud**

For each functional database, a six step process will be employed:

TABLE 9: STEPS IN THE PROCESS OF LINKING UID TO FUNCTIONS DATABASES

STEP		TIMEFRAME
1.	**LEGAL**: complete a legal review and revision (where necessary)	6 months
2.	**SYSTEMS**: complete a review of systems architecture and database structures	6 months
3.	**VALIDATION RULES**: develop validation rules to clean data using the UID and functional databases	2 months
4.	**DATA VERIFICATION**: using validation rules and links to the UID, clean existing data, fixing errors and removing fraudulent records	6 months, then continuous
5.	**ACCESS RULES AND LINKING**: develop data sharing rules for which information can be shared and under what circumstances	2 months then revised
6.	**PROVIDE ACCESS TO SERVICES,** by querying the UID and checking biometrics of customers	Ongoing

Some legal key legal changes have already been identified, such as:

- **Civil Registry**: At present, there is no obligation for parents to register a new-born child within a specific period of time. Such an obligation, as well as other reforms to civil registration, requires the amendment of the Civil Registry Code Law (10/2011 of September 14). A draft amendment has been prepared, and has been consulted upon since 2014. There is still time for this draft to be extended to include the concept of a Unique ID.
- **Voter Registration**: Revisions are required in Articles 8 and 23, and Articles 13 to 20 (means of identification required for voter registration, database elements, access to electronic information, responsibilities for data protection)
- **Law 12/2016 of November 14 (Social Security Contributions)**: With the Contributory Social Security Scheme a specific system for registry and data storage has been created, as well as the allocation of an identification number.

Strategically, it was necessary to prioritize which systems would first to introduce UINs to their systems.[23] Ministries and other organizations are divided into four groups:

TABLE 10: ROLLOUT PLAN FOR EACH GROUP (IMPLEMENTING STEPS 1 TO 6)

GROUP	ORGANIZATION	2021	2022	2023	2024	2025	%
Group I	Ministry of Social Solidarity and Inclusion, Veterans Affairs, Civil Service Commission; Ministry of Finance, Banks, Mobile phone operators (Payment systems)	❶	❷❸	❹❺	❻	❻	75%
Group II	Ministry of Justice, Ministry of Health	❶	❷❸	❹❺	❻	❻	50%

[23] Possible criteria included: (i) the ease of linking the functional database; (ii) the impact of linking the functional database, for example, whether it was involved in implementing payment systems; (iii) the number of records in the functional database (for example, the Voter ID database contains the most records); and (iv) links to organizations likely to be involved in registration.

GROUP	ORGANIZATION	2021	2022	2023	2024	2025	%
Group III	STAE (Voter ID)		❶	❷❸	❹❺	❻	50%
Group IV	Ministry of Education, other Ministries		❶	❷❸	❹❺	❻	25%

NOTE: % estimates the fraction of records to be verified by 2025; steps 1-6 refers to Table 9 above

4.1 UIN WITHIN PAYMENTS DATABASES (GROUP I)

Group I includes key private sector operators, including Banks (especially those involved in the registration process or those that may have a requirement to have a UID to access services, such as holding a bank account). This group also includes Ministries making payments to beneficiaries. The Ministry of Finance is essential as it collects a variety of fees and taxes (requiring identification). It also has a very strong IT presence.

Focusing on payment systems is expected to reduce possible identity fraud in the systems documented adjacently. Overall:

- It is expected that 75% of the current records in Table 11 will be validated by the UID system. This is equivalent to approximately 1.1 Million records
- All Group I legal and business process reviews (the analysis) will be completed in 2021 and 2022
- Validation will begin in 2023

TABLE 11: GROUP I PROJECTIONS FOR NUMBER OF RECORDS VERIFIED

SYSTEM	CURRENT RECORDS	75% OF CURRENT
1. Bank Accounts [1]	198,000	148,500
2. Sim Cards [2]	1,500,000	562,500
3. Electricity [3]	160,505	120,379
4. TIN (MOF) [4]	26,483	19,862
5. Bolsa Da Mae (MSSI) [5]	101,339	76,004
6. SAII (MSSI)) [5]	107,470	80,603
7. Retirement Benefits [3]	30,000	22,500
8. Civil Servant salaries [6]	30,000	22,500
9. Veterans Benefits [5]	28,123	21,092
Total	**2,181,920**	**1,073,940**

SOURCES; 75% is calculated as 0.75 × current records. [1] 40% of the adult population, based on https://fred.stlouisfed.org/series/DDAI01TLA642NWDB; [2] World Bank statistics; for sim cards only half of the 75% target is assumed; [3] Data from the COVID response plan; [4] SERVE data on total business registration up to 2019; [5] 2021 state budget; [6] Civil Service Commission data, Public Administrative Reform program. All figures are estimates.

4.2 UIN WITHIN MOJ AND MOH DATABASES (GROUP II)

One of the primary systems with which the UID system should inter-operate is the DMIS, which manages electronic civil registry information. Although the civil and digital ID systems have a different focus, they can mutually reinforce accuracy and coverage. For example, a newborn should have a legal identity from birth, and the UID system should know when someone has died, so their identity cannot be fraudulently assumed. There is currently a backlog of approximately 600,000 paper records for births, that need to be entered into the DMIS for the DMIS and UID systems to effectively communicate.

Group II includes the Ministry of Justice and the Ministry of Health. Overall:

FIGURE 18: TARGETED BACKLOG OF PAPER CIVIL REGISTRY RECORDS TO BE ENTERED INTO THE DMIS

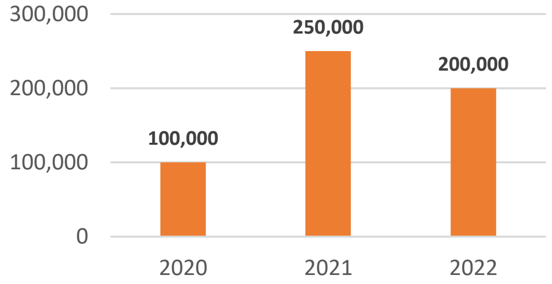


TABLE 12: GROUP II PROJECTIONS FOR NUMBER OF RECORDS VERIFIED

SYSTEM	RECORDS 2023	50% VERIFIED
1. Birth Registry [1]	1,088,390	544,195
2. Death Registry [2]	40,815	20,407
3. MOH health cards [3]	258,493	129,246
TOTAL	**1,387,698**	**693,849**

SOURCES; 50% calculated as 0. 5 × the estimated records in 2023. [1] 80% of the 2023 population were assumed to be in the DMIS.; [2] 10 per 1000 using a population of 1.3 Million; assumes deaths for 3 years as per https://data.worldbank.org /indicator/.DYN. CDRT.IN?locations=TL; [3] 19% use hospitals in a given year; https://academic.oup.com/inthealth/article/ 10/6/412/5051851

- It is expected that 50% of all births registered, deaths, and MOH records will have a UIN provided by the UID system. This is estimated to total about 700,000 records
- Legal and business systems analysis will be completed by the end of 2022
- Validation will begin in 2023

4.3 UIN WITHIN THE VOTER ID DATABASE (GROUP III)

Biometric information can greatly improve the accuracy of voter registration. The Ministry of State Administration is part of the UID technical committee which will work together throughout 2021 to agree on a joint strategy for implementing biometrics authentication. With the election to be held in early 2023, this timeframe may be too short to implement biometric voter registration for 2023. However, it will be available for future elections. This will be a strong opportunity to improve both the Voter rolls and improve the number of registered people within UID. Following the 2023 election, the UID and Voter ID databases will be cleaned and verified during 2024. With 845,000 records currently in the Voter ID database, verifying 50% will cover 422,500 records.

TABLE 13: GROUP IV PROJECTIONS FOR NUMBER OF RECORDS VERIFIED

SYSTEM	ESTIMATE 2024	25% OF CURRENT
1. National University [1]	2,000	500
2. Pre-School Students	94,853	23,713
3. Primary School Students [2]	259,795	64,949
4. Secondary Students	74,366	18,592
TOTAL	356,648	89,162

SOURCES; 25% is calculated as 0.25 × the estimated records. [1] based on a graduation of 500 students in 2020. [2] Education data from UNICEF (2017): "Timor-Leste Population and Housing Census 2015, Thematic Report Volume 11, Education Monograph 2017." Education figures in the UNICEF report were increased by 2.2% per year. All figures are estimates.

4.4 UIN WITHIN EDUCATION AND OTHER MINISTRIES (GROUP IV)

Group IV Ministries include the Ministries of Education and Interior. The UID system will be linked to: (i) university student records; (ii) pre-school, primary and secondary school records, and (iii) systems in use in other Ministries. Overall:

- It is expected that 25% of student and other information will have a UIN provided by the UID system. This is estimated to reach about 357,000 student records
- Legal and business systems analysis will be completed by the end of 2023

RESULTS

This component links the Unique Identification Number in the UID to functional databases, allowing them to access UID data and to better validate their data and removed duplicate identities. Expected results are as follows:

TABLE 14: COMPONENT #4 EXPECTED RESULTS

SYSTEM	2021	2022	2023	2024	2025
NUMBER OF SYSTEMS COVERED			9	12	15
ESTIMATED NUMBER OF RECORDS IN FUNCTIONAL DATABASE WITH UINs					
1. Bank accounts			49,500	49,500	49,500
2. Sim cards			187,500	187,500	187,500
3. Electricity			40,126	40,126	40,126
4. TIN (MOF)			6,621	6,621	6,621
5. Bolsa da Mae (MSSI)			25,335	25,335	25,335
6. SAII (MSSI: Support for the elderly and invalids)			26,868	26,868	26,868
7. Retirement Benefits (SSI)			7,500	7,500	7,500
8. Civil Servant Salaries (CSC)			7,500	7,500	7,500
9. Veterans Benefits (MNLCA)			7,031	7,031	7,031
10. Birth Registry				272,098	272,098

SYSTEM	2021	2022	2023	2024	2025
11. Death Registry				10,204	10,204
12. MOH health cards				64,623	64,623
13. Voter ID					422,500
14. National University					500
15. Ministry of Education					429,015
Total			**360,003**	**706,928**	**1,558,944**
Cumulative Records			**360,003**	**1,066,931**	**2,625,875**
COMPLETION OF KEY STEPS					
Step 1: Complete legal review	Group 1	Group 2	Group 3	Group 4	
Step 2: Complete systems review		Group 1	Group 2	Group 3	Group 4
Step 3: Design validation rules		Group 1	Group 2	Group 3	Group 4
Step 4: Complete Data verification			Group 1	Group 2	Group 3
Step 5: Provide access to other systems			Group 1	Group 2	Group 3

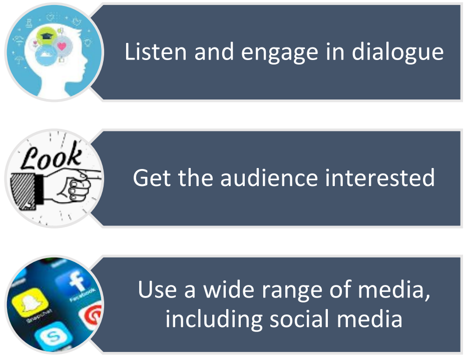
COMPONENT 5: OUTREACH AND COMMUNICATIONS

INTRODUCTION

Timor-Leste's Unique ID investment will be significant, but the returns can be multiple times that. Its success requires politicians, civil society, citizens and residents to be well informed about its benefits and procedures. All must actively participate, and people must want to register and must trust that their data is well protected. Without participation and trust, UID's will not succeed.

This strategy takes a modern communications approach. It moves from a traditional role of disseminating information ("informing people"), into a more strategic direction, where communication targets a change in specific behavior. This strategy also moves towards social media and aims to develop communications tools and channels that will engage the audience, where messages are developed from the audience's perspective and where these messages are delivered through the right mix of channels to capture the imagination and to motivate the audience to act. Communications plays a vital and supporting role in Components #1 to #4.

FIGURE 19: COMMUNICATIONS PRINCIPLES



Listen and engage in dialogue

Get the audience interested

Use a wide range of media, including social media

Component overview

The goals of this component and its key outputs are as follows:

GOALS

- **Motivate people to register**
- **Build trust in the security and privacy of the UID**
- **Motivate the private sector and Ministries to use the UID to verify their clients and use UINs in their functional databases**

OUTPUTS	
5.1	• Launch and brand the UID to gain government COMMITMENT
5.2	• Facilitate debate on privacy and data protection to BUILD THE TRUST of potential users
5.3	• Motivate people to REGISTER for UID
5.4	• Motivate public and private entities to INCORPORATE and use UID in their systems

Outputs 5.2-5.4 firmly link communications to three key areas of the plan: legal protections, registration, and development of functional databases while the first output provides foundational information.

5.1 LAUNCH AND BRAND UID TO GAIN GOVERNMENT COMMITMENT

The UID project is a whole-of-government approach requiring the commitment of multiple Ministries and Agencies. Without the support of key politicians, and ministerial staff, the initiative will not be successful. The project launch will extend over a period of several months and will aim to ensure the genuine acceptance and participation of key decision makers.

Messaging will focus on: (i) what the UID system is and how it will work; (ii) what the benefits of the UID system are; (iii) what is expected of each Ministry in the future; (iv) what data protection and security safeguards will be in place; and (v) the importance of open source software and vendor neutrality. To spread these messages a presentation will be made in each Ministry, supported by brochures, FAQs (frequently asked questions) and other printed materials. Most of these materials, together with a detailed identification of messages and audiences, were developed during the formulation phase of this strategy, with the support of UNICEF.

During the approval of this document, in early 2021, extensive consultation with civil society, the public and private sectors has taken place, including outreach to 37 Civil Society organizations, 15 Private Enterprise entities, including banks, mobile providers and the ICT industry, 22 Development Partners and International NGO's and 14 legal advisers within KTE member institutions. ensuring the quality and acceptance of the strategy.

Once the UID decree law has been passed 1 television and 1 radio spot will be designed introducing citizens to the concept of UID. Finally, during the "launch phase:"

FIGURE 20: LAUNCHING

- *Behavioral objective*: Ministries become committed to genuinely implement the UID
- *Key messages will explain*: what the UID is, how the UID will work, what are its benefits, what safeguards are in place ("UID: a gateway to services")
- *Channels*: Ministry presentations and materials; social media, television, radio to introduce UIDs to the public

- The UID will be branded[24]
- Facebook, Twitter and other social media accounts will be established
- The website uid.gov.tl[25] will be actively promoted (especially on social media)
- A help / information desk, initially under TIC Timor will be created

While the launching phase will provide an initial understanding, both government officials and citizens are unlikely to remember much of the details. It is not until elements of the UID system are further developed or become implemented that detailed knowledge will be actually required.

5.2 FACILITATE DEBATE ON DISSEMINIATION OF PRIVACY AND DATA PROTECTION TO BUILD THE TRUST OF POTENTIAL USERS

During 2021, in the development of the *Law Data Protection and Privacy*, UID managers will facilitate a discussion on the importance of privacy. Without having the public's confidence that their personal information is protected, few will want to register for the UID system. This debate provides a tremendous opportunity to explain the UID, and to gain the support of key intermediaries, that can promote registration of UIDs. Key stakeholders will include: (i) NGOs, especially those representing the

FIGURE 21: DATA PROTECTION

- *Behavioral objective*: Citizens and providers trust that data and privacy are protected
- *Key messages will explain*: background on the UID; how data will be protected; security measures ("your data will be safe and secure," "privacy first")
- *Channels*: conferences; social media, traditional media

[24] For example: "Secure your identity," "secure your rights;" "Trusted ID," "Trusted service;" "One ID for multiple access;" "UID making a better future;" "UID is the way to a better future." Alternatively, a national campaign for the public to name UID may be held to gather community involvement in UID.

[25] The site uid.gov.tl may be changed when the branding of UID is undertaken.

disadvantaged and poor; (ii) the legal community; (iii) churches; (iv) the media; (v) community leaders; (vi) youth organizations. Feedback will be provided through conferences, social media platforms and the traditional media.

Messaging will focus on: (i) background on the UID system (what, how and why); (ii) proposed legal safeguards and data protection; (iii) security measures.

Once the law is created, annual television, radio and social media will be used to describe safeguards and protections.

5.3 MOTIVATE CITIZENS TO REGISTER FOR A UNIQUE ID

Registration will be the most important period of time to motivate citizens to apply for a UID. While agents, who are providing registration services on an outsourced basis, are likely to use communications to encourage registration, the Government will still need to undertake significant initiatives to promote registration. This communication will be implemented on an annual basis beginning in early 2023.

Messaging will focus on: (i) what the UID system is and how it will work; (ii) what the benefits of the UID system are; (iii) how to register, in particular what documents to bring;[26] (iv) where to register and when, including how long registration is expected to take; (v) the conditions of registration (for example, if a payment will be made to the person registering); (vi) how accreditation will work; (vi) how information and privacy will be protected; and (vi) complaints and feedback mechanism;

Annually, these messages will be disseminated using 2 television shows and 12 monthly radio spots and ongoing social media campaigns. In addition, all Suco chiefs will be contacted and informed how to mobilize their residents. Email, social media, and text messaging[27] will be used to directly reach as many citizens as possible.

FIGURE 22: REGISTRATION

- *Behavioral objective*: Most citizens register for UID
- *Key messages will explain*: Why, how, when and where to register ("UID is your basic right," "Equality and privacy is ensured," "Get your UID now," "Call … for complaints and assistance")
- *Channels*: television and radio spots; Suco level visits and announcements; social media and text messages

5.4 MOTIVATE PUBLIC AND PRIVATE ENTITIES TO INCORPORATE UID INTO THEIR FUNCTIONAL DATABASES

To meet the objective of improving access to services, the UID system will need to link to individual identity systems in use across the public and private sectors. Linking to these systems, and establishing data exchange protocols, will require a deep cooperation between UID staff and each public and private sector service provider. As described in Component #4, systems can be linked and data verified, only after a legal and business process review is completed for each system. These activities require intensive participation from each service provider.

FIGURE 23: FUNCTIONAL DATABASES

- *Behavioral objective*: public and private sector organizations want to integrate the UID into their systems
- *Key messages will explain*: what is the UID and its benefits to each service provider; how will data be kept secure; what are the steps in linking to the UID ("Save money, eliminate fraud," "Get more clients")
- *Channels*: presentations, visits, handouts, brochures

[26] Where different groups will be registered in a different way, this will be explained.

[27] The communication and media survey conducted by UNMIT in 2011 shows community leaders followed by radio and television are consistently the most accessed and most trusted sources of information. Posters and banners received low or zero recognition. Digital 2020 datareportal.com reported there were 1.45 million mobile connections in Timor-Leste, 515,100 internet users and 410,000 social media user in January 2020. Facebook is by far the most common social media network in use.

It will only be during this very practical, analytical step that a true understanding of the nature and rationale of the UID system can be built. Communication will be essential to:

- Get the agreement of service provider as to their intention and timeline to link to the UID
- Motivate the provider to work with the UID team to revise legal and systems issues and to develop data exchange protocols and verification rules, on a timely basis
- Follow up the service provider to understand how well the system is working

The communications process will consist of:

1. Visiting each individual service provider (for example, a bank) and explaining what how and why the UID system can be useful, the process of utilizing the UID system and what is expected of the service provider, if it participates. This will consist of a presentation to managers followed by an agreement on a timeline of cooperation (for example, signing an MOU).
2. Getting feedback from the provider on how well the UID system is working

RESULTS

Expected results for communications initiatives are as follows:

TABLE 15: COMPONENT #5 EXPECTED COMMUNICATION RESULTS

ITEM	2021	2022	2023	2024	2025
LAUNCHING					
Hotline and complaints system in place		Q4			
Number of television shows/radio programs designed and aired to provide general information on UIDs	1/1	1/1	1/1	1/1	1/1
Number of Ministries where Ministers and senior management were provided information on the launch of the UID system	All				
LEGAL PROTECTIONS ON PRIVACY AND DATA EXCHANGE					
Number of NGOs, Churches, and civil society representatives consulted	100				
Number of social media posts on privacy and data protection		20	20	20	20
Number of television shows/radio programs designed and aired on data protections			1/1	1/1	1/1
REGISTRATION		160	160	320	320
Number of television shows/radio programs designed and aired to promote registration			1/12	1/12	1/12
Number of Suco level promotion activities implemented			160	160	80
Number of text messages sent promoting registration			500,000	500,000	250,000
FUNCTIONAL DATABASES					
Number of entities visited and presented with information on how to link to the UID			25	25	25

SUMMARY BUDGET

The total cost of the developing and implementing the UID system, from 2021 until mid-2025 is estimated to be $US 13.8 Million. Costs include management, human resources (staffing for registration and headquarters) and the procurement of equipment and software. Aggregate projected costs are summarized below while a detailed budget can be found in the annex.

FIGURE 24: COST COMPOSITION

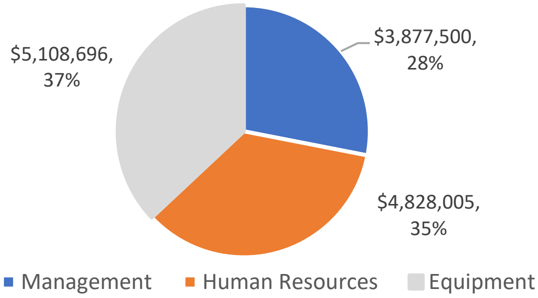


TABLE 16: PROJECTED COSTS BY MAIN CATEGORY (ALL YEARS)

ITEM	AMOUNT	%
1. MANAGEMENT	**$3,877,500**	**28.06%**
1.1. System Integrator and Project Management	$2,550,000	18.46%
1.2. Information, Education, and Communication (IEC)	$351,500	2.54%
1.3. Legal Costs	$50,000	0.36%
1.4. Training	$250,000	1.81%
1.5. Running a helpdesk	$136,000	0.98%
1.6. Software support to functional databases	$500,000	3.62%
1.7. Datacenter hosting charges	$40,000	0.29%
2. HUMAN RESOURCES	**$4,828,005**	**34.95%**
2.1. Mobile Registration	$1,511,814	10.94%
2.2. External Agents Registration	$1,073,156	7.77%
2.3. UID Agency Operation (Excluding registration)	$2,199,400	15.92%
2.4. Hiring Costs	$43,635	0.32%
3. **EQUIPMENT**	**$5,108,696**	**36.97%**
3.1. Servers and related items	$453,600	3.28%
3.2. ABIS & SDK	$1,440,000	10.42%
3.3. Other Hardware and Software	$525,600	3.80%
3.4. Team Vehicles	$468,000	3.39%
3.5. Registrar's Full Kit	$56,940	0.41%
3.6. Registrar's Basic Kit (alternative to full kit)	$41,340	0.30%
3.7. Mobile connectivity device (price for 4 years)	$56,160	0.41%
3.8. Robust Credential (With procurement and markups)	$1,596,123	11.55%
3.9. Authentication (with procurement & markup)	$34,800	0.25%
3.10. Backup Hardware and Disaster Recovery	$436,133	3.16%
TOTAL	**$13,814,201**	**100.00%**

Many of these costs (management, some equipment procurement) is likely to be funded by development partners, with other funding coming from the Sovereign Wealth Fund (CAFI) and possibly external financing (Worldbank, ADB).

UNIQUE IDENTITY (UID) SYSTEM

ANNEXES, OPERATIONAL PLAN AND BUDGET

2021 TO 2025

MAY 2021

VOLUME II

TRUSTED DIGITAL IDENTITIES TO UNLOCK SERVICES FOR ALL

ANNEX 1: PROS AND CONS OF THE 4 OPTIONS

This annex documents pros and cons of the 4 options considered for the UID system: (i) separate digital and civil identities; (ii) birth certificate required; (iii) digital identity within the civil registry; and (iv) the use of 1 column (the "Estonian Model). The Council of Ministers selected the first option, which is documented in the strategic plan.

TABLE 17: PROS AND CONS FOR OPTION #1 (SEPARATE DIGITAL AND CIVIL IDENTITIES)

PROs	CONs
■ Easy and inclusive registration ■ Less time and cost ■ Faster to clean other data bases of duplicates, fakes and ghosts ■ No dependency on Birth Registry ■ Minimalistic approach enables Privacy by design ■ Designed to work as a platform for other systems and databases (BI Card, Voter ID, Health, Education) to utilize the Biometric information in UID that is available to all. ■ Focused project objective, more likely to succeed. ■ Used in Philippines, India, Pakistan, Malawi, Togo, Tanzania ■ Most popular method now (Pacific countries) ■ Inclusive, fast & economical, allows registration of people with a birth certificate or a declaration from the local authority for those without a birth certificate ■ Internet is not needed to register people. Offline mode. ■ Legal Identity Administration remains with Ministry of Justice. MOJ can use the information in UID to provide improved BI Card (Smart BI) – using the biometric information in the UID system. ■ Similarly, STAE can use the UID biometrics for their Voter ID. ■ Can still register citizens' births at the same time as registering UID, but as a separate process, removes the dependency on Birth Registry and the MOJ DMIS system. ■ Will slowly improve the Birth Registry over time through data matching and removal of duplicates	■ Not necessarily a legal identity, it is a digital identity that can be linked to a legal identity. ■ Ministries still responsible for all Functional ID's, such as BI Cards, Voter IDs, Drivers Licenses. ■ Does not involve in simultaneously improving the Birth Registry system, as they are separate systems, however replacing the Birth Registry is encouraged.
COMPUTERIZATION	

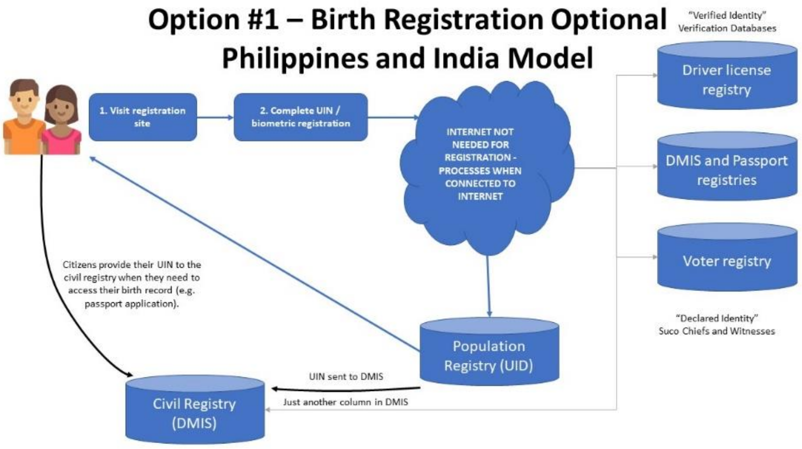

Option #1 – Birth Registration Optional
Philippines and India Model
"Verified Identity"
Verification Databases
1. Visit registration site
2. Complete UIN / biometric registration
INTERNET NOT NEEDED FOR REGISTRATION - PROCESSES WHEN CONNECTED TO INTERNET
Driver license registry
DMIS and Passport registries
Voter registry
"Declared Identity"
Suco Chiefs and Witnesses
Citizens provide their UIN to the civil registry when they need to access their birth record (e.g. passport application).
Population Registry (UID)
UIN sent to DMIS
Just another column in DMIS
Civil Registry (DMIS)

TABLE 18: PROS AND CONS FOR OPTION #2 (JOINT REGISTRATION)

PROs	CONs
■ It is a legal identity, as well as digital ID ■ Birth Registration is necessary, improving that registry ■ Consistent biographical information between the UID and Birth Registry database ■ Biometric information is registered in UID, and available to all.	■ Requires validation of a small set of civil registration biographical data, which may delay UID registration and will require MOJ to certify its paper and online registries ■ Requires significant upgrade of the DMIS and an internet connection to register people. No offline mode for the DMIS. ■ For records already in the DMIS, relies upon the accuracy of this data or its validation with paper records ■ Requires different procedures for: (i) people with electronic birth data (approx. 400,000); (ii) people in the paper-based birth registry but not in the DMIS (approx. 600,000); and (iii) people not registered (approx. 300,000). ■ Will only work with the FULL COOPERATION of the MOJ; otherwise option #1 would be used as a "Plan B" for registration
COMPUTERIZATION	

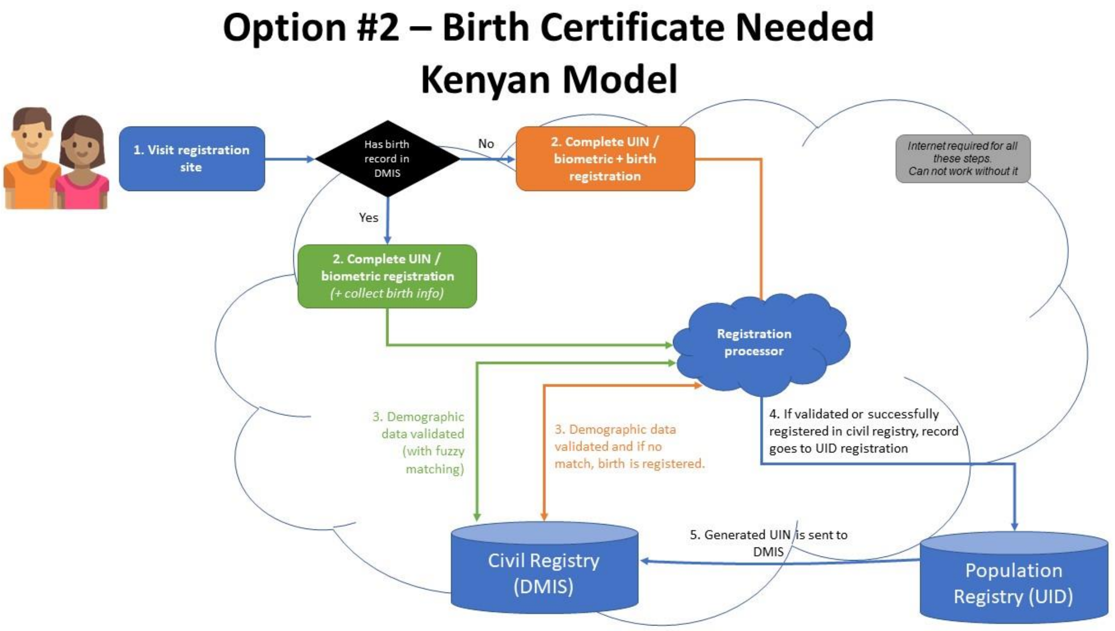

Option #2 – Birth Certificate Needed
Kenyan Model
1. Visit registration site
Has birth record in DMIS
No
Yes
2. Complete UIN / biometric + birth registration
Internet required for all these steps. Can not work without it
2. Complete UIN / biometric registration (+ collect birth info)
Registration processor
3. Demographic data validated (with fuzzy matching)
3. Demographic data validated and if no match, birth is registered.
4. If validated or successfully registered in civil registry, record goes to UID registration
5. Generated UIN is sent to DMIS
Civil Registry (DMIS)
Population Registry (UID)

TABLE 19: PROS AND CONS FOR OPTION #3 (ALL WORK UNDER THE DMIS)

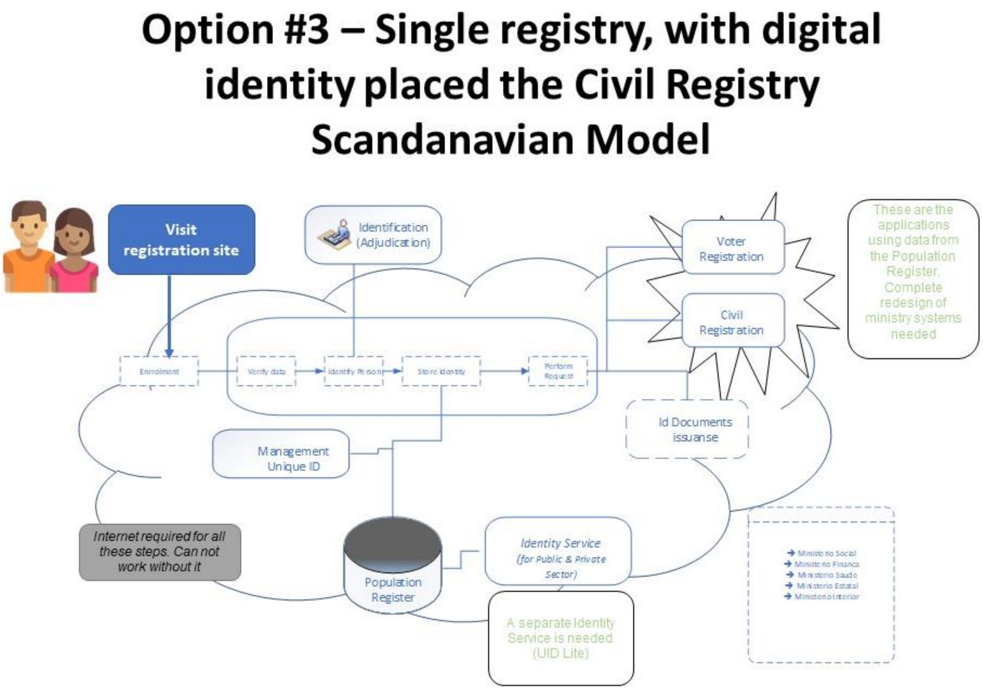
PROs

- It is a legal identity, as well as a digital ID
- Establish comprehensive registry that can be used for a wide range of administrative and statistical purposes
- Complete linkage of UID and Birth Registry database
- Implemented in Sweden, Norway, Denmark, Thailand (incomplete) - No Low Income or Developing country tried recently

CONs

- Extremely difficult to design and implement and to cost
- Substantial policy, technical and legal reforms likely to take years before registration can begin
- Requires very strong initial Birth Registry and State Capacity
- Requires an internet connection to register people. No offline mode
- Longer time to clean other data bases of duplicates, fakes & ghosts
- Creates dependency on Birth Registry system, importing its flaws
- Vulnerable to data theft due to access to and integration with multiple agencies
- Added personal information compromises privacy, expect legal challenges, Constitutional privacy clause

COMPUTERIZATION



Option #3 – Single registry, with digital identity placed the Civil Registry Scandanavian Model

Visit registration site
Identification (Adjudication)
Voter Registration
Civil Registration
These are the applications using data from the Population Register. Complete redesign of ministry systems needed
Enrollment
Verify data
Identify Person
Store identity
Perform Request
Management Unique ID
Id Documents issuance
Internet required for all these steps. Can not work without it
Population Register
Identity Service (for Public & Private Sector)
A separate Identity Service is needed (UID Lite)
Ministerio Social
Ministerio Financa
Ministerio Saude
Ministerio Estatal
Ministerio Interior

TABLE 20: PROS AND CONS FOR OPTION #4 (ONE COLUMN)

PROs	CONs
■ Capacity can be built more slowly. Costs are lower as the registration process does not require biometrics	■ Access to services are unlikely to improve as citizens would still need to provide various (rather than a single) paper certificate ■ More difficult to detect identity fraud ■ Less beneficial for the private sector

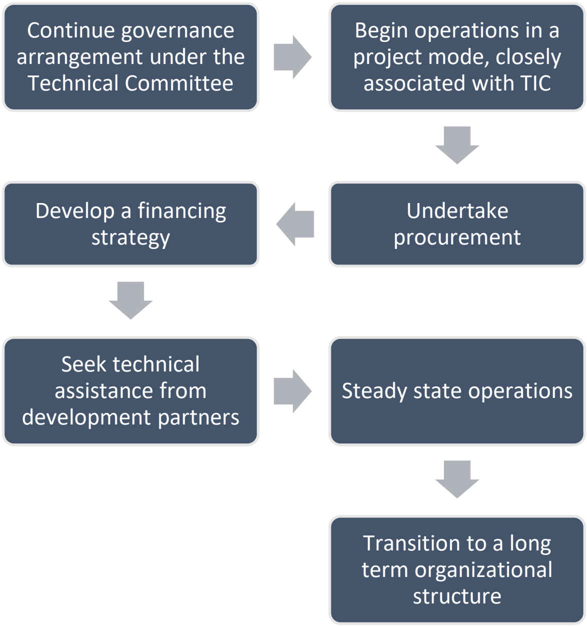
ANNEX 2: ORGANIZATIONAL STRUCTURES

FROM PROJECT TO MISSION STRUCTURE TO AGENCY

The success of the Unique ID will depend to a great extent on the organization which manages it.

Unique ID activities are currently managed under the Technical Committee, with project management undertaken by TIC Timor. During 2021 a temporary mission structure, closely aligned to TIC Timor, and overseen by the UID Technical Committee. Will be established. Over time the structure will be strengthened; it will gain experience; and it will be converted either into a separate agency, possibly under the MOJ, or will be incorporated into TIC. Key steps are outlined adjacently in Figure 25 and are described in turn.

FIGURE 25: KEY STEPS IN FORMING AN AGENCY


Continue governance arrangement under the Technical Committee
Begin operations in a project mode, closely associated with TIC
Undertake procurement
Develop a financing strategy
Seek technical assistance from development partners
Steady state operations
Transition to a long term organizational structure

Continue governance arrangement under the Technical Committee

The technical committee will become the Steering Committee to guide and direct the mission structure to implement the UID project. The Ministry of Transport and Communication, the National Institute of Social Security and the General Directorate of Statistics should be also included in the Technical Committee.

The expanded Technical Committee will establish a series of Inter-agency committees that will be set up to coordinate issues related to:

- **Legal** (to develop any legal instruments still required)
- **Technology** (supporting procurement and development of technology infrastructure, including software and hardware)
- **Communication support** (UID branding to gain government commitment, trust building, public awareness, public motivation to register, public and private organizations motivations to integrate UIN)
- **Registration and validation** (development of standards, processes, guidelines and plans for registration, both mass registration and steady state)
- **Use cases, authentication and functional database linkages** (identification and development of use cases, standards, processes, guidelines and credentials
- **Reporting,** coordination, decision escalation, modification of mandate, budgetary support, etc.

Begin operations in a project mode, closely associated with TIC

As the project starts, essential qualified staff will need to be in place. Job descriptions and staffing profiles will be developed and a core team will be hired. This team will oversee the system design definition, the procurement process, the system's development and integration phase, the registration pilots.

Undertake procurement

The mission structure will need to undertake a wide range of crucial and high profile procurement initiatives. UID in-house capacity will be assessed including for managing procurement processes and for leading the development and management of various solution elements. Public sector procurement regulations will be adhered to, and:

- Market analyses and vendor consultations will be organized
- A risk assessment will be conducted
- Procurement options will be defined including: (i) defining and designing each procurement component; (ii) deciding on the number of RFPs for vendor's procurement; (iii) defining procurement methods; and (iv) defining bidding procedures

Development Partner assistance in the procurement stage is recommended, to ensure that the requirements are properly identified and that the highest number of bidders can be included, reducing costs to the project. This will involve output deliverables identified in the RFP's rather than itemized lists. This has been shown in other countries to provide the greatest value for money and achieved innovative solutions. Both the World Bank and the Asian Development Bank has expressed interest in assisting in this process.

Develop a financing strategy for the Agency

The financial strategy will guarantee long-term fiscal and operational sustainability. The UID agency will expand sources of revenues stemming from providing authentication and eKYC transaction services. A policy decision will be adopted on the pricing of UID services.

The provision for fee structures (e.g., on a pay per transaction model) can be made for both government and private organizations and reflect the added value of each transactions, e.g., basic authentication (i.e., authentication of a Yes/No result) can be free; attribute verification (e.g., proof of age, or proof of place of birth) can be charged; eKYC including data retrieval (for instance a photo or an address) can be charged.

Initially, during the Mission Structure phase of UID implementation, the use of UID system will be free for public and private enterprises to ensure a strong uptake and implementation. As part of the transition of the project to steady state operations under an Agency or Directorate, wide consultations will need to be had to understand the impact and possible revenues generated by a pay per transaction model. All entities part of Unique ID will be heard and the most appropriate solution for the ongoing financial sustainability and usability of Unique ID will be implemented after 2025.

Seek technical assistance from development partners to support operations

Institutional arrangements for Development Partners/stakeholders will be established, including pooling, monitoring, review, advisory. Institutional arrangements will be reassessed on a regular basis to ensure alignment with the UID's mission and partnership benefit maximization.

The projected budget does not include areas that Development partners may assist, with National and International Advisers filling some roles that have been budgeted for within the Plan. This leaves the budget to be the upper limit of costs, but with Development Partner assistance, this is expected to be considerably lesser.

Steady state operations

Over time operations of the mission structure are expected to stabilize and become routine. During this time, the full UID team will be in place and coordination will be reinforced with internal and external partners to fine tune the operational plan before beginning of mass registration.

Transition to a long term organizational structure

The core team will identify additional human resources requirements to ensure transition to steady state operation.

ANNEX 3: UID AND DMIS SYSTEMS REQUIREMENTS

INTRODUCTION

The UID system will be the Government's central computerized registry of digital identity information. The strategic plan outlines the design principles of the UID, it's goal, and its five outputs, as summarized in Figure 26. This annex provides additional information on the UID and civil registration software and equipment needs.

FIGURE 26: COMPONENT #2 GOAL AND OUTPUTS

GOAL

Establish a well-functioning UID technology infrastructure that can record, link, secure, and validate digital identity information, including biographical information, biometric data, and a unique identification number

OUTPUTS

2.1	• Procure software, hardware and UID equipment
2.2	• Customize and operationalize the UID software
2.3	• Establish sound UID security protocols
2.4	• Creates software standards and data exchange protocols
2.5	• Upgrade the DMIS and Smart BI Systems

UID SOFTWARE AND EQUIPMENT

A key step in operationalizing the strategic plan will be the decision on which software to use. This section reviews the software's requirements and key functionality.

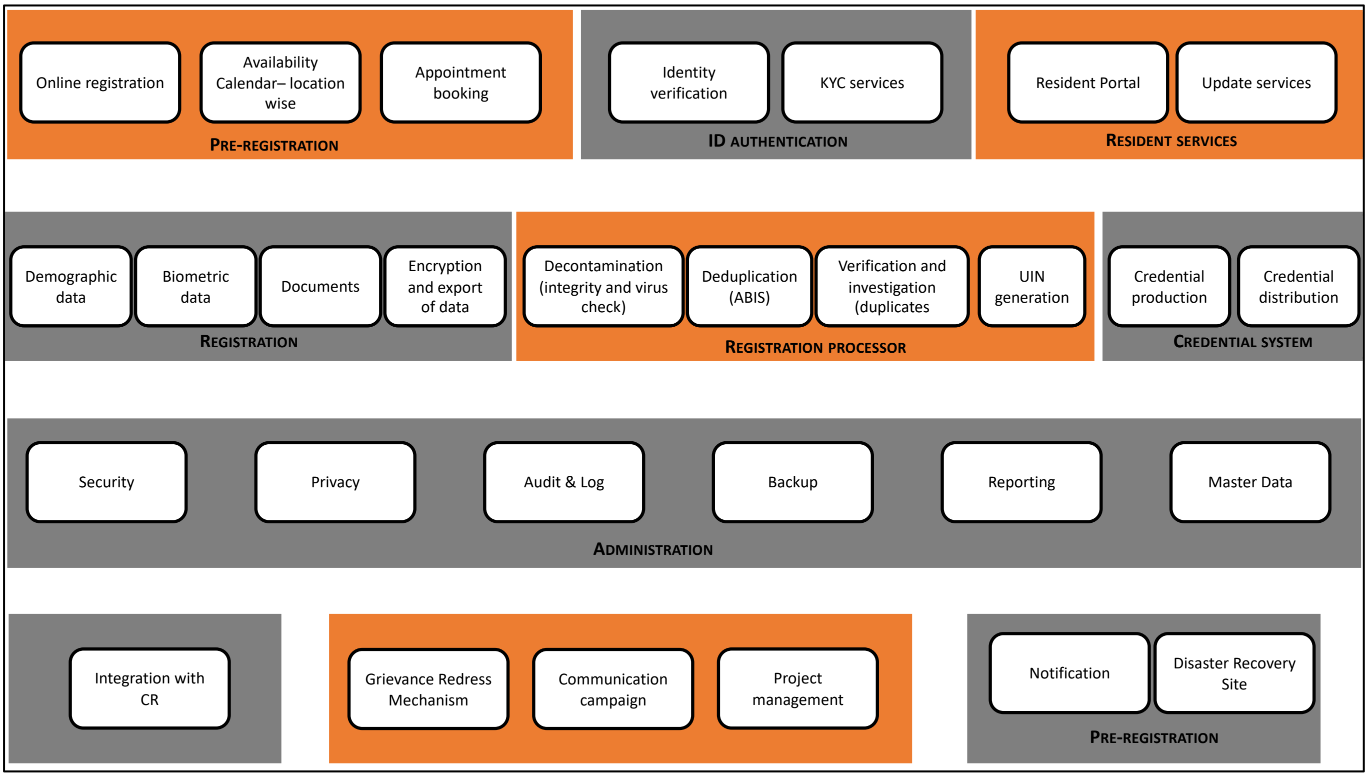
Functionality

The technical architecture and central ICT infrastructure will support the UID project and the operation of the UID system. The main functions of the systems are performed by the following technical modules:

- Data collection and registration;
- Processing of registration data
- Administration of the system including security of the infrastructure and data protection;
- Identity deduplication and verification;
- Credential production and distribution;
- Authentication and KYC services with external entities;
- Resident services;

These are described in turn. Additional supporting modules for the operation of the UID system will also be required, such as a Customer Relationship Module (CRM), Document Management, Knowledge Management, Project Management and Network Management.

FIGURE 27: NECESSARY MODULES AND FUNCTIONALITY OF THE UID SOFTWARE



Functionality: general considerations

The UID system will adopt international standards (e.g., ISO, NIST, IEC) to enable machine-to-machine communication, facilitate interoperability with external systems and avoid technology and vendor lock-in.

Technical standards will establish specifications and procedures in terms of the operation, maintenance and reliability of materials, products, methods and services, including for the regulation of the capture, encryption, storage, transmission, and use of identity data as well as the biometrics, the format and features of identity credentials and authentication protocols. Technical standards include:

- Biometrics' image standards apply to capturing face, eyes or fingerprint images
- Biometrics' data interchange format standards and biometrics' interface standards are both necessary to achieve full data interchange and interoperability for biometric recognition in an open systems environment
- 2D bar codes standards commonly apply to PDF417 and QR code in ID systems

The UID system will use open-source software to the maximum extent possible, in order to encourage and develop in-house technical capacity, ensure business continuity and ownership of the technology of the central ID infrastructure. Proprietary solutions and commercial software will be purchased only when not viable otherwise for the UID system.

Early on, the UID team will conduct a detailed assessment of the functional scope and the expected capacity of the system to inform further requirements.

The UID will identify technical profiles necessary for developing, integrating, operating, maintaining and upgrading the central infrastructure.

The initial development of the UID system will be supported by an external system integrator with demonstrated experience to ensure the best quality of the initial version of the deployed system.

Internal technical teams will benefit from trainings from the external system integrator during the initial development phase to develop sufficient skills and know-how to further operate, maintain and upgrade the system with only limited external support.

It will be a requirement that the system integrator ensures that the internal UID team can provide most levels of support of the UID system by 2025, with the system integrator only needed for high level or very complex support issues by that time. This "Timorisation" of the UID system is of critical importance and will ensure the long-term sustainability of the UID system.

The UID agency will nominate agencies to certify adoption of standards by all third parties authorized to use its system including registration and authentication agencies. The certification will cover human resources, devices, applications and network.

Functionality: data collection and registration

The system will collect demographic data, biometric data, and documents. It will capture, encrypt and export data, in line with the following requirements

TABLE 21: DATA COLLECTION AND REGISTRATION REQUIREMENTS

TYPE OF DATA	SPECIFICATION / FUNCTIONALITY
Biographic Data	■ The UID system will adopt a data minimization approach where only sufficient biographic data to establish the identity will be captured ■ The UID system will capture the name, date of birth, place of birth and, potentially, the names of the parents for those under 13 years old (Not mandatory for those with no recognized parents)
Biometric Data	■ The UID system will adopt a data minimization approach where only sufficient biometric data to establish the identity will be captured ■ The UID system will capture a facial image, fingerprints and possibly iris data (subject to testing in the pilot phases for assessment of quality) ■ The UID system will provide for robust exception handling mechanisms in relevant cases (e.g., in case of missing hands or eyes or loss of fingerprint definition in manual workers)
Documents	■ The UID will minimize the number of documents mandatory for registration. Verification documents may be scanned or photographed for record purposes ■ The UID system will optionally collect phone number and/or email address for communication and/or authentication purposes ■ The UID system will optionally collect a location for the person to collect their Secondary ID Credential ID card, such as a Suco Office
Capture, encryption and export of data	■ The individuals will be able to verify the accuracy of the registration data entered ■ A UID registration framework will be designed with standards and protocols to be adopted by internal and external registration agencies to connect and access the UID System. ■ The registration client application will capture and validate demographic and biometric data. The client will work online and offline to support registration in remote, rural and unconnected areas with provision for batch mode upload of files to the server for processing. The client application will be device agnostic and will work on standard workstations. ■ Data will be encrypted at the source and end to end both at rest on the client application and in transit during data uploads

Functionality: registration processor

Registration processing will consist of decontamination, deduplication (ABIS), verification and investigation (of duplicates), and the generation of an UIN. Most deduplication systems (ABIS) are proprietary software, which will be the largest (and likely only) proprietary software component in the UID system. The ABIS system providers have exclusive algorithms that are used for the 1 to N matching of biometric data. This introduces a significant licensing cost to the UID system. To reduce the dependence on this proprietary systems, an open source alternative will be developed in conjunction with the use of the proprietary software, allowing for the UID system to reduce its reliance on the expensive software, with the intention of replacing or minimizing its use significantly.

This will be done in line with the following requirements.

TABLE 22: DATA COLLECTION AND REGISTRATION REQUIREMENTS

FUNCTION	DETAILED SPECIFICATION
Decontamination	■ All data uploaded to the central system will undergo an integrity and virus check prior to being added to the central database
Deduplication (ABIS)	■ The backend servers will be architected for high demands of 1 to N biometric deduplication ■ Innovative techniques of hashing, indexing, distributed processing and in memory databases using multiple-biometric modes will be deployed to achieve desired performance ■ Multimodal deduplication systems could provide for higher level of assurance when used simultaneously ■ To ensure sustainability of UID system, alternatives to proprietary ABIS systems will be developed in tandem to adhere to the principle of reducing any non open-source software. ■ Multimodal deduplication systems could provide for a robust exception handling mechanism in exceptional case (e.g., if individual has no hand and main deduplication system is fingerprints)
Verification and investigation (duplicates)	■ The UID system will endeavor to guarantee that each identity is unique, secure and accurate ■ Manual adjudication procedures will be implemented to verify identity uniqueness or duplication in cases flagged by the system ■ The UID system will provide for robust exception management protocols at ID validation, including for cases related to the absence of particular biometric data (e.g., fingerprints in the case of an individual without hands), changing biometrics, and cases of infants without a name at the time of registration
UIN generation	■ The individuals will be able to verify the accuracy of the registration data entered ■ A UID adoption framework will be designed with standards and protocols to be adopted by external registration agencies to connect and leverage the UID System. ■ The registration client application will capture and validate demographic and biometric data. The client will work online and offline to support registration in remote, rural and unconnected areas with provision for batch mode upload of files to the server for processing. The client application will be device agnostic and will work on standard workstations ■ Data will be encrypted both at rest on the client application and in transit during data uploads

Functionality: administration

Administration will help administer the technology platform of the UID and its operations including, security, privacy, audit and log, backup, reporting, and management of master data. Key requirement will include:

TABLE 23: ADMINSITRATION REQUIREMENTS

FUNCTION	DETAILED SPECIFICATION
Security	■ A data protection and cybersecurity plan will be implemented, including regular vulnerability assessments and response plans tested to responds to security attacks and threats ■ All personal identifiable information will be encrypted and inaccessible to unauthorized internal and external parties ■ The security infrastructure will provide protection from logical/physical attack including server security (firewall, intrusion prevention and detection systems), network, client security encryption. Physical security will also include strict access management system to prevent unauthorized access to the UID precinct, theft of blank credentials, and access to datacenter room, and procedures for the protection against fire, etc. ■ The UID system will provide for the ability to quarantine and isolate data when attacked or compromised ■ The UID system will not permit records to be deleted ■ Role based access control- assign rights over UID resources based upon roles ■ Account setup- creation/modification of registrar and authenticating/user agency accounts
Privacy	■ The UID system will adopt a privacy-by-design and privacy-by-default approach ■ The UID system will store only minimal biographic and biometric information and will neither aggregate data nor profile or track individuals ■ The UID system will collect a minimal set of metadata about the registration process ■ All personal identifiable information will be encrypted and inaccessible to unauthorized internal and external parties, ■ The system will regulate access to personal data by authorized personnel and prevent access to personal data to any unauthorized personnel ■ Access to citizen data will be based on citizen’s consent ■ The UID system will consider deploying tokenization or other cryptographic methods to reduce correlation of identity ”accounts” and data sharing by relying parties
Audit and Log	■ The UID system will ensure that all events are auditable and not repudiable ■ The UID will enable to track every access to the UID system and session activities ■ The UID system will have fraud detection mechanisms to detect identity theft and cybercrimes using audit trails
Backup	■ A backup strategy and procedure will be defined, implemented and audited to guarantee business continuity
Reporting	■ Visual decision support tools such as GIS, charting, etc. ■ Reporting will be customizable and allow for the creation of a variety of tools to pilot operation, monitor the system and track registration progress
Master Data:	■ This will be the most critical element of the system as it will contain the raw data of all residents ■ It will hold data of all residents but will contain only the minimal set of fields sufficient to verify identity

Functionality: the credential system

Credential production will adopt a data minimization approach where only sufficient data to verify the identity will appear on the credential and/or be accessible via machine readable mechanism. Requirements for the production of main and secondary credentials as well as credential distribution, are as follows.

TABLE 24: REQUIREMENTS FOR CREDENTIAL PRODUCTION AND DISTRIBUTION

FUNCTION	DETAILED SPECIFICATION
Main credential production	■ The UID system will issue a unique ID number (UIN) to each registered individual after the identity verification process ■ The UIN will be a randomized and unique number that contains no personal information ■ The UIN will contain control digits ■ The UIN or a tokenized UIN will be used as a key amongst external databases belonging to various service providers ■ The use of the UIN in external database will not require the latter to transform their existing infrastructure other than the elements required to comply with cybersecurity, data protection and privacy requirements
Secondary credential production	■ The definition of secondary credentials, if any, will respond to a thorough cost-benefit analysis and provide high value for money ■ Technical features of physical credentials will need to be defined including its material (paper or plastic), level of security features, if any (level 1, level 2 or level 3), integration of machine-readable elements (2D barcode or QR code, chip) ■ It is anticipated in the budget that the Secondary Credential will be a Plastic PVC card with overt security, a facial picture and a QR code ■ Digital credentials could include mobile ID (UID on a smartphone), virtual ID (revocable tokenized version of the UIN for front-end online authentication) ■ The fields appearing on credentials, the language used, and the fields accessible via machine-readable mechanism will be defined (in line with the data minimization approach)
Credential distribution	■ A credential distribution strategy for the UIN and, for secondary credentials will be established and will assess potential distribution channels including, but not limited to collection points and downloads. ■ For physical credentials, the UID will rely on one or more reliable logistics partner for the shipment of physical credentials to the issuance site ■ In addition to communication by a physical channel, the UIN number may also be communicated to individual owners digitally ■ UID can consider various distribution option: one option is the UID authority alone generates the UID number and distributes it; the other option can be each enrolment agency receives a file containing the UID Number against the data fields captured at the time of registration and each organizes delivery to its beneficiaries/customers with freedom to add information related to its services (customer ID by bank, TIN number by Revenue Agency) a combination of the two may also be considered.

Functionality: identity verification services

The UID system is primarily an authentication provider. Its principal function in a steady state is to provide means for individuals to prove their identity, i.e., to demonstrate to a service provider that "I am who I claim to be" with a sufficient level of assurance that the service provider will accept the result of the authentication process. Requirements will be in terms of central infrastructure, architecture and standards; authentication; know your customer; use cases, the business model, as defined below.

TABLE 25: REQUIREMENTS FOR VERIFICATION SERVICES

FUNCTION	DETAILED SPECIFICATION
Central infrastructure, architecture and standards	■ The backend servers will be architected for large peak loads from authentication requests ■ The UID system will allow for integration and interoperability with a growing number of external databases subject to applicable data protection and privacy regime ■ A UID registration framework will be designed with standards and protocols to be adopted by user agencies to connect and access the UID System ■ Authentication and data exchange services will be regulated by an access rule, linking and data exchange framework ■ The authentication system will be designed to serve the population, with particular attention on the poor and other vulnerable populations, by making it easier for them to authenticate once registered in the UID system ■ A mechanism to link the UID system with service delivery systems will be put in place to ensure that targeted benefits reach intended beneficiaries: UID enables ID verification while the service delivery system guarantee eligibility to a service. The mechanism will be supported by ad hoc in policy and regulation
Authentication	General requirements ■ The authentication services will be developed with customer's convenience, security and privacy as core principles this will have implications on data used for authentication as well as data sharing policy ■ Authentication will always be grounded on the individual's informed consent, with use of data restricted to the specific purpose for it is obtained ■ The UID system will provide for robust exception management protocols for authentication ■ A set of rules will be implemented to restrict the sharing of the UIN for other than intended purposes to avoid the uncontrolled and unsecure dissemination of the UIN Potential offline authentication methods ■ Secondary physical credential taken at face value ■ Fingerprint, face, or iris 1:1 matching against QR barcode of physical credential Potential online authentication methods can include either or both demographic and biometric authentication using APIs exposed by the UID system. Recommended methods include: ■ Fingerprint, face, or iris 1:1 matching against UID database ■ OTP though SMS ■ Biographic data matching
KYC services	■ The UID will provide for eKYC services and allow for attribute retrieval in line with the data protection and privacy legislation ■ KYC service will allow for sharing limited demographic data and a photo, in compliance with the law, following a successful authentication and consent of the user (online)

FUNCTION	DETAILED SPECIFICATION
User agencies, use-cases and technical assistance for implementation	■ The UID authentication services will be made available to user agencies subject to applicable data protection and privacy regime ■ A set of policy will be formulated to regulate the selection and authorization of user agencies in a transparent and consistent manner ■ A core team on use cases/domain experts (banking, telecom, social protection, process re-engineering, etc.) will be constituted ■ A strategic plan on use cases and applications will be designed to promote the adoption of UID's services ■ Consultations with public and private sector, regulators and policy makers will be held to ascertain demand and requirements ■ Use cases will specifically target the poor and vulnerable populations by facilitating their access to basic services and benefits. The demand for authentication services will grow with citizens perceiving its utility. ■ The adoption of UID will have a direct correlation with subsequent enrolment. A positive and mutually beneficial self-reinforcing cycle will develop between adoption and enrolment. ■ Budget implications entailed by the necessary re-engineering of the user agencies' infrastructure to connect and leverage the UID system could stonewall the adoption of UID services and will be mitigated by a support and technical assistance strategy. ■ Given that process re-engineering is a specialist domain, the ID authority will identify strategically important use cases, build in-house teams to work on them and reach out to actual user agencies to adopt them and where necessary assist in adoption ■ The UID system will provide support and technical assistance to user agencies to understand, deploy, test and use the interconnect standards and protocols defined in the UID adoption framework. ■ The UID system will provide support and technical assistance to user agencies to leverage biometric ID for cleaning their databases and using the UID services for authentication.

Functionality: resident services

Requirements for the provision of resident services includes operating a resident portal and updating data and addressing lost ID cards, as follows.

TABLE 26: REQUIREMENTS FOR VERIFICATION SERVICES

FUNCTION	DETAILED SPECIFICATION
Resident portal	■ The UID system will make available a resident portal for individuals to access information, track their requests, provide feedback on services, etc. ■ The UID will allow users to update data online in a secure manner (address, phone number, etc.
Update data, Lost ID card	■ UID number is a lifetime number but biometric and demographic information may change over time. ■ The UID system will allow for the update free of charge of biometrics for children until it stabilizes around 13 years old, or more generally after an injury leading to the alteration of the characteristics of the individuals. ■ The UID system will allow for the update free of charge of changing biographic information including the as name (e.g., after marriage), the address, the mobile phone numbers and the email. ■ There may be errors in the fields that occur during registration for UID in need of correction. User agencies may require updates as a condition to receive benefits/service. Service centers will need to be authorized for residents to make updates with or without documentary evidence. This may also include a biometric authentication prior to processing the request. Online update facilities could also be considered.

CIVIL REGISTRATION (DMIS) SOFTWARE AND EQUIPMENT

Although the UID system and the DMIS (Demographic Management Information System) are separate systems and although the project does not depend on the DMIS, **the unique ID system would greatly benefit from the adoption of new, open-source civil registry software** and an expansion in the number of citizens with birth certificates, for the ongoing sustainability of UID. The UID system will also depend on data on deaths to deactivate a UID record.

DMIS / Electronic Civil Registry Functionality

As documented in the strategic plan, the DMIS faces significant problems and urgently requires both and an upgrade of the civil registry system and changes to ensure interoperability with external systems, in line with the following requirements.

TABLE 27: REQUIREMENTS FOR AN IMPROVED COMPUTERIZED CIVIL REGISTRY SYSTEM

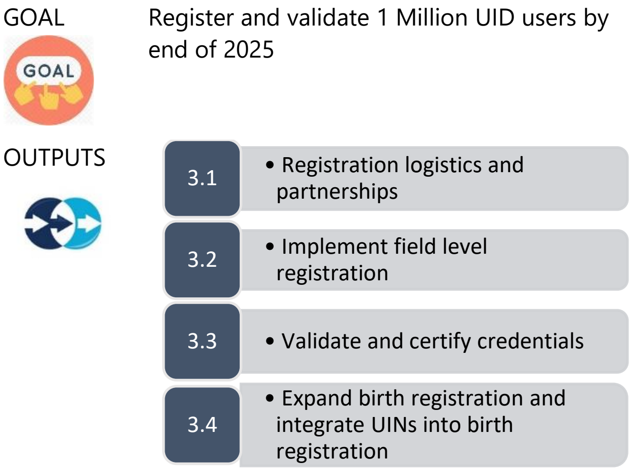
FUNCTION	DETAILED SPECIFICATION
Upgrade of the CR system	■ The CR system will aim to ensure universal access to birth and death registration, to facilitate access to birth and death certificate and to improve the registration of other life events. ■ The CR system will adopt open standards and open-source software to the maximum extent possible, in order to promote technology and vendor neutrality and foster in-house capacity ■ The CR system will operate both offline and online
Interoperability with external systems	■ The UID system will enable exportation of parents/legal guardians to smooth birth registration process ■ The UID system will be expanded to birth registration and integration of the UIN into the birth certificate ■ A UIN will be given from Birth. The UID system will get the birth details from CR system. CR system triggers the creation of a UID. This will be automatic for any birth registered in the CR system ■ The CR system will allow for real-time update to deactivate UIN of people registered dead. The UID system will not remove a record upon a person's death; it will only mark it as 'deceased' and deactivate it for purposes of authentication ■ The CR system will be linked with vital statistics system to improve life events notification and update

ANNEX 4: REGISTRATION

INTRODUCTION

To be successful, the UID system will need to quickly achieve a critical mass of users. In the beginning, large-scale registration campaigns will be necessary. This will make identification accessible to substantial segments of the population, within a short timeframe. The goals of this component and its four outputs are summarized adjacently.

FIGURE 28: COMPONENT #3 GOAL AND OUTPUTS



GOAL

Register and validate 1 Million UID users by end of 2025

OUTPUTS

3.1 • Registration logistics and partnerships

3.2 • Implement field level registration

3.3 • Validate and certify credentials

3.4 • Expand birth registration and integrate UINs into birth registration

REGISTRATION LOGISTICS AND PARTNERSHIPS

Intensive planning will be required to implement the registration process.

The mission structure will include a registration unit that will manage registration and authentication services. This unit will consult with different stakeholders as it develops a more detailed registration plan. An M&E system will be put in place to track progress and record the growth and development of the project for management as well as historic purposes.

During 2021, an inclusion strategy will be developed to specifically target the most vulnerable populations. Its principles are as follows:

TABLE 28: PRINCIPLES OF AN INCLUSION STRATEGY

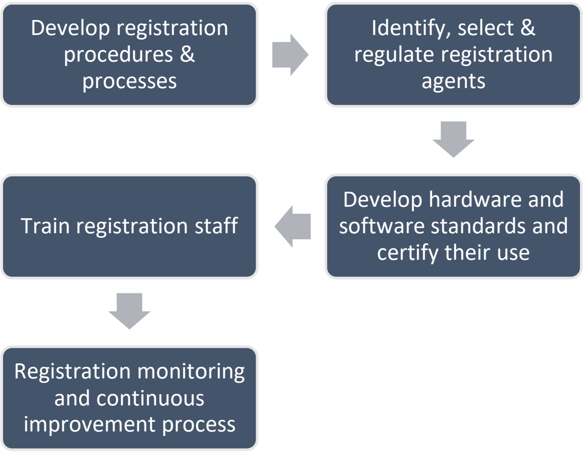
PRINCIPLE	DETAILS
Direct and indirect costs to registration will be minimized	■ Registration in the system and the issuance of the credential will be borne by the UID system and be free of charge for the population ■ The registration will ensure that the indirect time spent to go to the enrolment center, cost of transportation, lost wage, cost for individuals to register will be minimal ■ The UID system will minimize requirements for registration (including breeder documentation) by providing a choice of documents to register to ensure inclusion ■ Incentives (mainly positive, but also negative) will be defined and enforced to encourage registration

PRINCIPLE	DETAILS
Outreach groups will be shortlisted, and adequate strategies will be developed	■ UID will work with civil society, development partners and enrolment agencies to shortlist outreach groups (hard to reach and marginalized populations) and define mitigation plans ■ Specific communication campaigns will be conducted to target specific vulnerable groups. ■ The poor and vulnerable populations will be specifically targeted by facilitating their access to basic services and benefits. The demand for registration services will grow with citizens perceiving its utility. ■ Registration centers will include the use of "fast lanes" for specific populations (elderly people, pregnant women, disabled, etc.) ■ UID will ensure access to services for people speaking only local languages/dialects by providing for use of local languages to register as well as avail subsequent services including a multi-lingual helpline
Poor and hard to reach groups will be addressed	■ Enrolment agencies will collaborate with organizations working with the poor and hard to reach groups; ■ Co-resident enrolment with heads of families and businesses enabling registration of family members and employees with their address proof; ■ Financial institutions where the urban poor often borrow from can serve as enrolment points; ■ NGOs and on Profits can be used to educate on the benefits of the UID, for actual enrolment and to help endorse identity for people without documents
The special needs of children will be addressed	■ UID will leverage child related programs and/or locations like immunization centers, child care centers, schools and educational institutions to conduct enrolment. ■ Registration procedures will be designed to allow for registration against the biographic details of the parents and primary caregivers as children seldom have their own documents
The special needs of women will be addressed	■ Special efforts will be made to enroll women by enlisting the support of women's group and organizations working for women. ■ Registration procedures will be designed to allow for registering people without existing documentation, as women as often under-documented.
The special needs of the disabled will be addressed	■ UID will cooperate with associated NGO's and rights groups to target, inform and enroll differently abled persons. ■ Registration procedures will be designed to allow those without fingers to enroll without fingerprints capture
The special needs of other marginalized groups will be addressed	■ UID will formulate a plan to take in consideration specific requirements for the registration of the homeless, individuals in shelter, remand homes or asylum, transgender and indigenous people. ■ The language to be used for information campaigns will be adapted to match local languages, if applies.
The special needs of infants will be addressed	■ As capturing the biometrics of infants and children is challenging, the biographic details of parent(s) may be recorded. Biometrics will then be collected when the child turns 13 years old. This can be enforced with by an expiry date attached to the UID number.

REGISTRATION

Registration will collect the minimal biographical information, and biometric data needed for UID registration. Any other information that may be collected such a mobile phone number, ID collection point, registration metadata and similar will also be stored securely. No costs will be paid by applicants. Prior to rollout, the registration will be piloted; this will include optimizing the sensitivity of biometric uniqueness checks. The pilot may show adjustments will be needed in the registration process. The project and procurement plans will need to be flexible enough to allow for such changes. Implementation will include the 5 broad steps outlined in Figure 29.

FIGURE 29: KEY REGISTRATION STEPS


Develop registration procedures & processes
Identify, select & regulate registration agents
Develop hardware and software standards and certify their use
Train registration staff
Registration monitoring and continuous improvement process

Develop registration procedures and processes

Registration procedures and processes, online and offline, will be standardized throughout the Timor-Leste for both UID contract staff and external registrars. The registration process will comprise preliminary verification, data collection, data verification by the enrollee, process completion confirmation. Verification procedures will be defined and entail document-based, witnessed-based and/or community-based verifications.

Data collection of demographic and biometric data will follow the data minimization principle and be standardized (except in case of exception handling situations)

The application request will be submitted, either singly or in batches, to the UID central infrastructure to perform identity deduplication and verify uniqueness in the central database in real-time when operating online or asynchronously when operating offline.

The UID will define a laydown a data transfer plan/partners to ensure access to nearest facility for batch upload in case of offline registration. It will envisage pre-registration solutions to facilitate registration this may include prefilled forms.

The UID will define an exception management strategy to deal with registration and authentication failures/exceptions.

Identify, select and regulate external enrolment agencies and internal registrars

Outside agents, such as Municipalities, other Ministries, banks, and private sector firms will be contracted to register people to receive their UID. This decentralized approach will need to be closely regulated, to ensure the protection of citizens' rights and the accurate collection and transfer of data.

Concerning staff of the agency / mission, UID staff registrars will be trained and provided with certified equipment, and adequate vehicles to conduct registration. They will be paid a fixed salary plus and extra fee per validated registration to encourage efficiency and maximum effort.

Leveraging external agencies (public and/or private), in particular those with large customer and/or beneficiary bases will make initial enrolment rapid. And, relying on multiple agencies (public and/or private) will provide individuals willing to register with choice of service provider, which will fuel competition and may positively impact on the registration quality and cost. These external agencies will provide trained and certified staff and equipment complying with required standards and infrastructure to conduct the registration. They will be paid a fixed fee per validated registration. The UID agency/mission will appoint a certification agency to ensure that only certified agents will be allowed to undertake registration work.

Develop hardware and software standards and require and certify their use

UID agency / mission will design, test, pilot and scale registration and authentication application software. This will be based on the standards that it has defined, including technical requirements and protocols for hardware, software and processes used for registration. The UID agency/mission will be as technology-agnostic as possible when establishing the technical requirements for enrolment kits. Occasional inspections will be undertaken with respect to external enrolment agencies to ensure they comply with all standards, protocols and certifications to connect to and leverage the UID system. The UID agency will oversee the full devices certification process.

For its own equipment, the UID agency will define a procurement plan for registration devices and will assess various options (e.g., purchasing, leasing, hiring, etc.).

Train registration staff

Training programs will be defined for registrars and supervisors. Training will be provided by an external training agency / organization. Training will cover:

- System administrators overseeing the mass registration; training will ensure they can use adequate monitoring tools for better planning and risk mitigation
- Registration staff; training will ensure they can adhere to the registration step-by-step process, exception handling, behavioral attitude and customer service, and the general understanding of the UID system

Registration staff will demonstrate adequate qualification via specific exam and/or training completion

Registration monitoring and continuous improvement process

Meta data will be collected during registration process to enable the monitoring of enrolment trends and patterns. Visual reporting tools and GIS software will be used to enhance planning of the registration. The meta data to be collected during enrolment will:

- Be defined following on an outcome-based selection and be minimized to limit privacy risks
- Be leveraged to monitor compliance with registration process and flag cases where registration personnel are taking shortcuts

The UID agency will carry out periodic checks to ensure data quality coming from all registrars. This quality check will include online verification including through crowd sourcing, verification against scanned documents, physical documents verification, process audits inspection, and leverage monitoring, mystery shopping, and meta data.

ANNEX 5: SECURITY

INTRODUCTION

Currently, every ministry, every bank and many other institutions, public and private, that provide services to the public collects personal identifying information on the people it interacts with. Each entity collects significant information, with the purpose of using this information to correctly identify the person as who they say they are. This usually consists of the person's Name, Sex, Date of Birth, Place of Birth, Current Address, Past Addresses, Parents Name, and often as well as Parents Date of Birth, Parents Place of Birth, Grandparents Names, height, weight, blood type, and other personal private and sensitive information.

Most of this information is collected beyond the need for the entity to deliver its services, but solely to provide a method of identifying the person. This information is stored within these entities in an often insecure manner, with little ability for the citizen to access personal data as a right given by the constitution of the RDTL, Article 38. The level of security of this information is a problem, with the ability of the entity to add, change and/or delete that information with perhaps no auditing, and not informing the citizen of the changes being made. This creates risks to citizens' personal information. It is likely that citizens' data are displayed in various forms such as in paper and digital formats, which open ways for the misuse of citizens' data, creates multiplication of unnecessary data and duplication of efforts and support. For example, when attending a bank or ministry, and you have to provide a photocopy of your ID each time, this is often stored insecurely in a back room for anyone in that area to access.

A main purpose of Unique ID is to resolve some of these issues around identifying people and how to authenticate that the person is who they say they are. Unique ID can provide this identifying and authentication to the population, public and private entities will no longer need to collect unnecessary personal information. Unique ID will take that requirement away from the other entity, and Unique ID can do this with as minimal personal identifying information as possible. Name, Date of Birth, Place of Birth and biometrics. All people residing within Timor-Leste will then have a single identity, a Unique ID, that would hold this identifying information, rather than perhaps 100's of entities.

This will provide a significant improvement in the Security and Privacy of personal information for all people of Timor-Leste.

MAIN PRINCIPLES

The key method to provide a safe and secure system for Unique ID is to work with a Privacy and Security by Design methodology. This means that the solution chosen must have the privacy and security of the Citizens foremost in the design, build and implementation of Unique ID.

The preferred method is to implement an open-source platform and embrace open standards. This will allow Timor-Leste to own the system fully, with the ability to change and customize the system to its needs, as the GoTL will have the source code to do so.

Data Sovereignty will be maintained by ensuring all data remains in Timor-Leste and is housed in country.

TIC Timor has a Fiber Optic network ring around Timor-Leste, so the Unique ID centers in Municipalities are not reliant on Internet, as they will be able to access the system directly via the high-speed TIC Fiber Optic links.

The UID Mission Structure would undertake an exhaustive software search to do a comparative analysis on the software that is available, taking into account the preference for Open Source and Open Standards software.

Once the software is chosen, the UID Project Team would then commission a system integrator to assist the team in developing this Open-Source software to the needs of Timor-Leste, with the Privacy and Security by Design being a guiding principle.

A benefit of using Open-Source is the potential to develop in new directions and evolve to meet new challenges. Additionally, competition is encouraged when a vendor-neutral, open platform is adopted as the core of an identity solution.

Competition brings down the cost and avoids lock-in to a particular proprietary technology, or a particular vendor. As it is open source, any Vendor can bid on supporting Timor-Leste as the Systems Integrator. This competition helps reduces costs and addresses the question of financial sustainability in the long run.

Unique ID will address user privacy with a consent framework that lets the individual user choose what to share and when. For example, to provide e-KYC details or to pre-fill forms, the user must consent to this by submitting their biometrics, such as a fingerprint, for the UID system to validate. From a security perspective, all personally identifiable information is encrypted both in motion and at rest and is inaccessible to internal and external parties without user consent. All flow of such information is in trusted environments only, with the data never stored unencrypted.

The goal of the Unique ID system is to provide a safe, secure and trusted mechanism for Citizens to identify themselves to Government and Private entities. This will include data deduplication across multiple government systems to remove ghost and fake identities.

This also creates an ICT separation between Unique ID and other government systems. The Unique ID interfaces to the other systems are hardened and secure and provides minimal information sharing. This is the "Just another column" method proposed in the Estonian Report.

This is a sound practice, as generally, the systems within Ministries are often out of date, unpatched and often out of support. The Unique ID system will be providing the "firewall" functionality between these systems to ensure that in the event of a Ministry system being compromised, no other systems are affected, including Unique ID. This why a new system is needed, rather than trying to overlay new features onto existing out of date software, which would be a much higher security risk than software that was designed for Privacy and Security from the beginning.

This Security by Design process will provide a strong basis for ensuring the integrity of the systems and notifications of possible issues as they are occurring. This strong basis of security means that possible issues of hacking, illicit data access and data theft has a much higher chance of being discovered and addressed quickly.

Having an Open-Source and Open Standards Unique ID system means that the core code of the system is visible, allowing experts, civil society and citizens to review and improve the security of the core system as time goes on. The closed source alternative is a black-box, the GoTL would have no visibility into the core of the system, and GoTL would just have to trust the Software Provider that everything is ok.

Information Security for these systems will be an ongoing process, with improvements needed continuously to ensure the safest, most secure system possible for Timor-Leste.

As shown in Annex 3, there will be significant safeguards to be implemented regarding security, privacy, auditing and logging and backup

This is not a complete list with full impact and vulnerability assessments needing to be undertaken at numerous points during the discussion, design, build and implementation of the Unique ID System.

These items will significantly decrease the risk of data privacy and security breaches, as it has been seen across the world that it is usually the Public and Private Institutions that is breached, not the Unique Identity entity. This is due to the UID entity having one sole objective, to provide a safe, secure identity platform that has the trust of the people. Ministries and other entities have other priorities, being the delivery of the service for which is its purpose (i.e. providing health services by Ministry of Health). This often means IT Security and the systems around the protection, privacy and auditing of personal information is under-funded and does not have the visibility within the organization it should.

However, with the Unique ID entity, this is its sole purpose. Without the trust of the people whose data it holds, it cannot function. This means that managing the security and privacy of the data held by the Unique ID system is paramount. This is achieved by ensuring that Privacy and Security of data is considered at every step in Unique ID's operation. Issues arise when the security and privacy of data is not prioritized and is not funded to allow it to occur, and when there is limited or absence of law to protect data and privacy. Unique ID will have these aspects as a priority and the software will have security and privacy embedded into its design which will make data breaches less likely.

No system can guarantee that it is 100% safe and truly hacker proof. Even Angela Merkel, the Chancellor of Germany, had her phone hacked. The UID system will be designed to ensure that if there is any security threat, either by external hackers, or by internal disgruntled staff, the system has protective measures to ensure the data is secure. All events will be auditable and non-repudiable (cannot be reversed), Records can never be deleted, and vulnerability assessments will be routinely performed, including automated 24/7 monitoring of all systems.

Unique ID system will consider implications of a data breach beforehand, through encryption of all data, possible tokenization of the Unique ID number and other mechanisms, in the event of a breach at either a Ministry, private enterprise, or the UID entity itself, the impact on the citizen will be minimized as possible, due to the minimal information stored within UID. Comparing this to a potential current data breach in a Ministry which collects significantly more personal information than UID.

Unique ID has a specific purpose, the identification and authentication of people within Timor-Leste, citizens, foreigners, stateless, refugees, those with no ID. It can only do this with the support and trust of the people.

As such, ensuring the safety, security and privacy of the data of the people whose information it holds is the key to Unique ID succeeding. The data held will be protected and kept securely.

ANNEX 6: COST BENEFIT ANALYSIS

This annex estimates costs and benefits of the Unique ID project. Several scenarios are investigated, each showing the project to have a high internal rate of return under a wide range of assumptions. Under a conservative baseline estimate, **the UID project has an internal rate of return of 21% when using a 10-year time horizon and 24% when using a 15-year time horizon**, making the project extremely favorable. Using a 5% discount rate over the first 10 years of the project the project will deliver benefits of $US 6.3 Million on a net present value (NPV) basis. Over a 15-year period, the NPV increases to $US 12.9 Million.

COSTS

From 2022 to 2025 the project will cost $13.8 Million. Costs are divided into equipment, staffing, and management costs. Over the 15-year time horizon (2022 to 2036), costs average $US 3,005,245 per year, though these fluctuate between $US 2 Million and $US 6 million depending on the purchase of equipment (valued at $US 4 Million and assumed to be replaced every 5 years). The composition and evolution of costs are depicted adjacently.

Several sources of funding are possible, including:

- Funding from CAFI
- Development partner grants and technical assistance
- Revenues raised by charging fees for identity verification

The analysis calculates total costs and benefits over the lifetime of the project, not the costs and benefits based on the Government's contribution to the project. Since no loans are envisioned, the source of funding does not affect calculations.

DEFINITION OF BENEFITS

The UID project is expected to have the following main benefits:

TABLE 29: TYPES OF BENEFITS OF THE UID

TYPE	DESCRIPTION
Time savings to citizens	Currently citizens are required to provide a great number of documents to validate their identity and are required to make numerous trips to access services. The UID system will reduce this hardship.
Service provider savings when doing ID checks.	The online UID system will save time and effort for the service provider to validate the identity of a service recipient. This will lead to a cost savings in terms of staff time, paper work, etc.
Savings by reducing and identifying fraud	The UID system, and its connection to a wide range of databases can identify duplicate entries and payments, inconsistencies and fraud.

The following are not benefits and are therefore not included in the calculation:

- **Staff wages**. Though job creation and the receipt of wages is a benefit to an employee it is accounted for as a cost of generating the UID service

- **Revenues received by the Government**. Anything received by the Government would be paid by a company. In general, any payment which distributes resources from one party to another is not part of a cost benefit analysis.

FUNCTIONAL DATABASES GENERATE THE BENEFITS

Benefits (defined above in Table 29) are generated through the functional databases---driver's licenses, banks identification, veterans benefits, and others. The UID provides the link and means of verifying digital identify across these databases. In all, by 2036 it is projected that about 5 Million records will be linked to the UID. The number of records accessed for ID verification determines the success of the project. The table below provides a detailed estimate of the number of records in each database that will be linked to the UID over time.

FIGURE 30: NUMBER OF RECORDS IN ALL FUNCTIONAL DATABASES

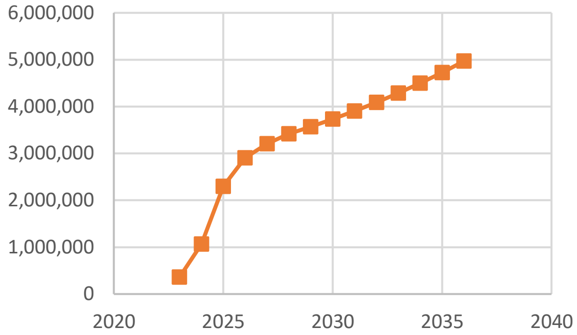


TABLE 30: PROJECTED NUMBER OF RECORDS IN DIFFERENT FUNCTIONAL DATABASES

CUMULATIVE RECORDS	2023	2024	2025	2026	2027	ANNUAL INCREASE ONWARD
Bank accounts	49,500	99,000	148,500	154,440	160,618	4.00%
Sim cards	187,500	375,000	562,500	618,750	680,625	10.00%
Electricity	40,126	80,252	120,378	125,193	130,201	4.00%
TIN (MOF)	6,621	13,242	19,863	20,658	21,484	4.00%
Bolsa da Mae (MSSI)	25,335	50,670	76,005	76,005	76,005	0.00%
SAII (MSSI: Elderly & invalids)	26,868	53,736	80,604	81,410	82,224	1.00%
Retirement Benefits (SSI)	7,500	15,000	22,500	23,400	24,336	4.00%
Civil Servant Salaries (CSC)	7,500	15,000	22,500	22,725	22,952	1.00%
Veterans Benefits (MNLCA)	7,031	14,062	21,093	20,038	19,036	-5.00%
Birth Registry		272,098	544,196	816,294	835,069	2.30%
Death Registry		10,204	20,408	30,612	31,316	2.30%
MOH health cards		64,623	129,246	193,869	205,501	6.00%
Voter ID			422,500	432,218	442,159	2.30%
National University			500	1,000	1,500	4.00%
Pre-School Students			23,713	47,427	71,140	2.30%
Primary School Students			64,949	129,898	194,846	2.30%
Secondary Students			18,592	37,183	55,775	4.00%
Drivers Licenses				38,333	76,666	4.00%
Land Registry				19,166	38,333	4.00%
Tax and Duties				19,166	38,333	5.00%
Total	**357,981**	**1,062,887**	**2,298,047**	**2,907,784**	**3,208,117**	

CALCULATING BENEFITS OF THE UID

The following assumptions were used to generate a base scenario to calculate the estimated rates of return.

	ASSUMPTIONS	VALUE	DESCRIPTION
1	Population 2022	1,400,000	
2	Population growth	2.3%	
	Used to calculate the value of time saved for the service user		

	ASSUMPTIONS	VALUE	DESCRIPTION
3	Value of one hour saved	$0.74	Based on a GDP of $US 2 Billion
4	Hours saved for the client for each new record in a functional database	3	Assumes time is only saved during the registration process
	Used to calculate the cost savings of the service provider		
5	Cost saved to the service provider (per ID check)	$1.00	
6	Number of ID checks per existing record / year	1	Assumes ID is checked 1 time per year for each existing record
	Used to calculate the benefits of fraud prevention		
7	% of fraudulent IDs (new functional DB records verified)	2.0%	
8	Value saved from a fraudulent transaction	$100.00	
9	Equipment lifetime	5 years	Affects total costs and the cost schedule

IRR CALCULATIONS AND SENSITIVITY ANALYSIS

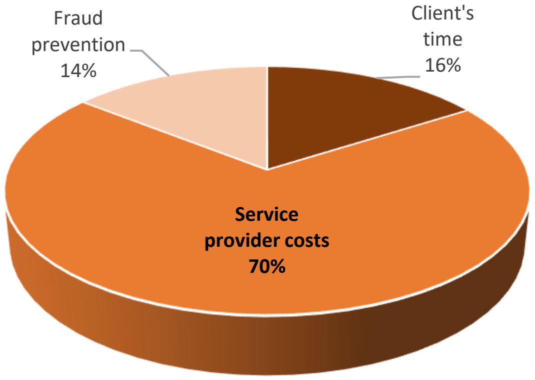
Under the above baseline assumptions, the internal rate of return is 21% over a 10-year period. Most of these benefits (Figure 31) are in the form of cost savings to the service provider, who requires few documents and document checks, less paper work, fewer staff, etc.).

The number of records in which digital ID is verified is the most important factor in the success of the UID project. Table 31 (below) provides a sensitivity analysis, calculating the internal rate of return of the project under various assumptions.

TABLE 31: SENSITIVITY OF THE IRR UNDER DIFFERENT ASSUMPTIONS

ITEM	IRR
Assumed number of records by 2031	
3 Million	11.6%
3.9 Million (baseline)	21.1%
5 Million	29.8%
Hours saved by the client per new transaction	
1 hour	8.9%
3 hours (baseline)	21.1%
5 hours	33.7%
Value of fraud per record	
$50	12.8%
$100 (baseline)	21.1%
$200	38.1%

FIGURE 31:COMPOSITION OF BENEFITS



ANNEX 7: ACTIVITY PLAN AND SCHEDULE

An implementation schedule for Unique IDs, as well as the budgeted cost of each activity can be found below.

	2021				2022				2023				2024				2025			
COMPONENT/OUTPUT/ACTIVITY	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
1. Legal & Institutional		🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
1.1. Create a unique ID project		🟧	🟧	🟧																
1.1.1. Complete operational plan		▨																		
1.1.2. Draft a project document and submit to CAFI		▨																		
1.1.3. Establish a Mission Structure			▨																	
1.1.4. Project becomes operational				▨																
1.1.5. Operate as a project					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
1.2. Create Laws to Protect Citizens' Data and Privacy		🟧	🟧	🟧	🟧	🟧														
1.2.1. Complete the drafting of a Data Privacy and Protection Law		▨																		
1.2.2. Approve the Data Privacy and Protection Law				▨																
1.2.3. Draft a Cyber Crime and E-Commerce Law				▨																
1.2.4. Approve a Cyber Crime and E-Commerce Law						▨														
1.2.5. Develop a Cyber Security policy						▨														
1.3. Strengthen the legal environment surrounding legal identity			🟧																	
1.3.1. Draft and approve a Unique ID decree law			▨																	
1.4. Creation of a Mission Structure & UID Agency			🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
1.4.1. Full UID team hired			▨																	
1.4.2. Market analysis and vendor consultations organized			▨																	
1.4.3. Risk Assessment conducted				▨																
1.4.4. Procurement & system development strategy developed			▨																	
1.4.5. Form a Mission Structure					▨															
1.4.6. Function temporarily as a Mission						▨	▨	▨	▨	▨	▨	▨	▨	▨						
1.4.7. Create a National ID Agency															▨					
1.4.8. Function as a National ID Agency																▨	▨	▨	▨	▨
2. UID System Development																				
2.1. Procure Software and Equipment				🟧	🟧															
2.1.1. Equipment and software procurement plan completed				▨	▨															
2.1.2. Assessment of possible UID software completed					▨															
2.1.3. System integrator identified					▨															
2.1.4. Primary and disaster recovery datacenters identified					▨															
2.2. Customize and Operationalize UID Software						🟧	🟧	🟧	🟧											
2.2.1. UID software system selected, customized, tested and ready for pilot registration operations						▨														

	2021				2022				2023				2024				2025			
COMPONENT/OUTPUT/ACTIVITY	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
2.2.2. Internal technical team trained						▨	▨	▨	▨											
2.2.3. Service contract for UID software support signed						▨														
2.3. Establish UID Security and Privacy Protocols				🟧																
2.3.1. Data protection and cybersecurity plan and vulnerability assessment and response completed and tested				▨																
2.4. Standards and Data Exchange Protocols									🟧											
2.4.1. ISO standards Data exchange and software protocols in place									▨											
2.5. DMIS Enhancement and BI Cards								🟧	🟧	🟧	🟧									
2.5.1. Feasibility of CRVS open source software completed								▨												
2.5.2. Upgraded CRVS in place									▨	▨	▨									
2.5.3. Detailed cost analysis SMART BI cards completed											▨									
3. Registration and validation						🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
3.1. Registration Logistics and Partnerships						🟧	🟧	🟧	🟧											
3.1.1. Registration plan and logistics completed (including development of knowledge management system)						▨	▨													
3.1.2. Incentive plans defined and enforced						▨														
3.1.3. Certification process for outsourced registration designed								▨	▨											
3.1.4. Registration agencies approved									▨											
3.1.5. Training certification program designed									▨											
3.1.6. Consultations on registrations held						▨	▨	▨												
3.2. Implement Registration of 1 Million Persons							🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
3.2.1. Registration process piloted							▨													
3.2.2. Toll-free help line created							▨	▨												
3.2.3. Residential portal developed							▨	▨												
3.2.4. Implement full registration									▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3.3. Validation and Credentials								🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
3.3.1. Robust exception management protocols at ID validation established								▨												
3.3.2. Manual adjudication procedures defined								▨												
3.3.3. New BI card developed by the MOJ, using information from the UID												▨	▨							
3.3.4. New BI Card issues and in operation														▨	▨	▨	▨	▨	▨	▨

	2021				2022				2023				2024				2025			
COMPONENT/OUTPUT/ACTIVITY	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
3.4. Expand and Upgrade Birth Registration										🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
3.4.1. Procedures for delayed naming established										▨										
3.4.2. Revised procedures in operation											▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
4. Use Cases & Functional Databases			🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
4.1. Group 1 - Ministry of Social Solidarity and Inclusion, Veterans Affairs, Civil Service Commission; Ministry of Finance, Banks, Cellphone operators (Payment systems)			🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
4.1.1. Step 1: Complete legal review			▨	▨																
4.1.2. Step 2: Complete systems review					▨	▨	▨	▨												
4.1.3. Step 3: Design validation rules					▨	▨	▨	▨												
4.1.4. Step 4: Complete Data verification									▨	▨	▨	▨								
4.1.5. Step 5: Provide access to other systems									▨	▨	▨	▨								
4.1.6. Group 1 systems in full operation													░	░	░	░	░	░	░	░
4.2. Group 2 - Ministry of Justice, Ministry of Health					🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
4.2.1. Step 1: Complete legal review					▨	▨	▨	▨												
4.2.2. Step 2: Complete systems review									▨	▨	▨	▨								
4.2.3. Step 3: Design validation rules									▨	▨	▨	▨								
4.2.4. Step 4: Complete Data verification													▨	▨	▨	▨				
4.2.5. Step 5: Provide access to other systems													▨	▨	▨	▨				
4.2.6. Group 2 systems in full operation																	▨	▨	▨	▨
4.3. Group 3 - STAE (Voter ID)					🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
4.3.1. Step 1: Complete legal review					▨	▨	▨	▨												
4.3.2. Step 2: Complete systems review					▨	▨	▨	▨												
4.3.3. Step 3: Design validation rules									▨	▨	▨	▨								
4.3.4. Step 4: Complete Data verification									▨	▨	▨	▨								
4.3.5. Step 5: Provide access to other systems													▨	▨	▨	▨				
4.3.6. Group 3 systems in full operation																	▨	▨	▨	▨
4.4. Group 4 - Ministry of Education, other Ministries									🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧	🟧
4.4.1. Step 1: Complete legal review									▨	▨	▨	▨								
4.4.2. Step 2: Complete systems review													▨	▨	▨	▨				
4.4.3. Step 3: Design validation rules																	▨	▨	▨	▨
4.4.4. Step 4: Complete Data verification																	▨	▨	▨	▨
4.4.5. Step 5: Provide access to other systems																				
5. Outreach and Communications				🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦	🟦
5.1. Launch and Brand UID to Gain Government Commitment				🟧	🟧	🟧	🟧													

	2021				2022				2023				2024				2025			
COMPONENT/OUTPUT/ACTIVITY	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
5.1.1. Information, Education & Communication (IEC) strategy consultative group established				░	░	░														
5.1.2. IEC strategy developed				░	░	░														
5.1.3. Inclusion strategy developed				░	░	░														
5.1.4. Public engagement and system branding strategy developed				░	░	░														
5.1.5. Facebook, Twitter and other social media accounts will be established					░	░														
5.1.6. The website uid.gov.tl will be actively promoted (especially on social media)					░	░														
5.1.7. Hotline and complaints system in place							░													
5.1.8. Television shows/radio programs designed and aired to provide general information on UIDs					░	░														
5.1.9. Ministries where Ministers and senior management were provided information on the launch of the UID system					░	░														
5.2. Facilitate Debate on and Dissemination of Privacy and Data Protection to Build the Trust of Potential Users					▓	▓	▓	▓	▓											
5.2.1. NGOs, Legal Community, Churches, Media and Community Leaders consulted					░	░	░	░	░											
5.2.2. Social media posts on privacy and data protection					░	░	░	░	░											
5.2.3. Television shows/radio programs designed and aired on data protections					░	░	░	░	░											
5.3. Motivate Citizens to Register for a Unique ID							▓	▓	▓	▓	▓	▓								
5.3.1. Television shows/radio programs designed and aired to promote registration							░	░	░	░	░	░								
5.3.2. Suco level promotion activities implemented							░	░	░	░	░	░								
5.3.3. Text messages sent promoting registration							░	░	░	░	░	░								
5.4. Motivate Public and Private Entities to Incorporate UID into their Functional Databases													▓	▓	▓	▓	▓	▓	▓	▓
5.4.1. Entities visited and presented with information on how to link to the UID													░	░	░	░	░	░	░	░
5.4.2. Obtain feedback from the provider on how well the UID system is working													░	░	░	░	░	░	░	░

ANNEX 8: DETAILED BUDGET

The detailed budget estimate is as follows. Estimates were developed on the basis of the best available information and substantial research. It will be subject to changes in plans and fluctuations in terms of inflation and market prices.

TABLE 32: DETAILED BUDGET (TOTAL ACROSS ALL YEARS)

ITEM	AMOUNT	%
1. MANAGEMENT	**$3,877,500**	**28.06%**
1.1. System Integrator and Project Management	*$2,550,000*	*18.45%*
1.1.1. External Consultancy firm for Project management support (including drafting requirements documents, supporting procurement process, ensuring Project Management quality) during 2 years	$600,000	4.34%
1.1.2. Travels	$60,000	0.43%
1.1.3. SI support for system development		
1.1.3.1. System Integrator support for SW development, integration and maintenance (MOSIP)	$1,260,000	9.12%
1.1.3.2. System Integrator support for Open Source ABIS development	$315,000	2.28%
1.1.3.3. System Integrator support for SW development, integration and maintenance (Open CRVS)	$315,000	2.28%
1.2. Information, Education, and Communication (IEC)	*$351,500*	*2.54%*
1.2.1. Preparation and execution of awareness raising campaigns and debate on privacy and data protection	$50,000	0.36%
1.2.2. Preparation and execution of awareness raising campaigns to boost registration (benefits of registration for population, registration process and requirements, etc)	$150,000	1.09%
1.2.3. Preparation and execution of awareness raising campaigns for government stakeholders, third parties and service providers	$80,000	0.58%
1.2.4. Development and distribution of information materials for target audiences	$60,000	0.43%
1.2.5. Development of service delivery materials for notification system and staff of ID	$11,500	0.08%
1.3. Legal: Support for drafting reform (ID law, privacy and data protection law, cybersecurity, cybercrime, eCommerce	*$50,000*	*0.36%*
1.4. Training	*$250,000*	*1.81%*
1.4.1. Contract staff training for mobile registration	$50,000	0.36%
1.4.2. External agents training - "train the trainers"	$50,000	0.36%
1.4.3. UID IT team capacity building (via MOSIP/Open CRVS customization training)	$75,000	0.54%
1.4.4. UID agency trainings	$75,000	0.54%
1.5. Helpdesk: Full time equivalent staff for helpdesk - population / registrars' support - during 4 years	*$136,000*	*0.98%*
1.6. Functional Databases: Funds for adjusting and changing the functional databases to allow for UIN (SI, HW, etc.)	*$500,000*	*3.62%*
1.7. Datacenter hosting charges	*$40,000*	*0.29%*
2. HUMAN RESOURCES	**$4,828,005**	**34.95%**
2.1. Mobile Registration	*$1,511,814*	*10.94%*

ITEM	AMOUNT	%
2.1.1. Total salary for contract staff (registrars + drivers)	$732,900	5.31%
2.1.2. Total per diems	$523,125	3.79%
2.1.3. Total cost of incentives	$255,789	1.85%
2.2. External Agents Registration	*$1,073,156*	*7.77%*
2.2.1. Total cost of fees for registration by external agents	$1,023,156	7.41%
2.2.2. Audit (external providers compliance verification costs)	$50,000	0.36%
2.3. UID Agency Operation (Excluding registration)	*$2,199,400*	*15.92%*
2.3.1. Staff category 1 (Office and clerical workers)	$36,750	0.27%
2.3.2. Staff category 2 (Service workers)	$55,650	0.40%
2.3.3. Staff category 3 (Technician)	$297,500	2.15%
2.3.4. Staff category 4 (Junior professional)	$525,000	3.80%
2.3.5. Staff category 5 (National Professional officer)	$472,500	3.42%
2.3.6. Staff category 6 (Managers and national advisors)	$392,000	2.84%
2.3.7. Staff category 7 (International advisors and CEO)	$420,000	3.04%
2.4. Hiring Costs	*$43,635*	*0.32%*
3. EQUIPMENT	**$5,108,696**	**36.98%**
3.1. Servers and related items	*$453,600*	*3.28%*
3.1.1. Servers to run custom applications to be developed by SI	$86,400	0.63%
3.1.2. Database Servers	$64,800	0.47%
3.1.3. Servers required to run REG applications	$57,600	0.42%
3.1.4. Servers required to run AUTHENT apps (manager and matching)	$57,600	0.42%
3.1.5. Perso prod servers	$172,800	1.25%
3.1.6. Additional servers for other software environments (e.g. test, pre-prod etc.)	$14,400	0.10%
3.2. ABIS & SDK	*$1,440,000*	*10.42%*
3.2.1. ABIS Product License	$540,000	3.91%
3.2.2. Bio SDK - Server side (for Auth)	$120,000	0.87%
3.2.3. Bio SDK - Client side	$240,000	1.74%
3.2.4. Annual maintenance - Support	$540,000	3.91%
3.3. Other Hardware and Software	*$525,600*	*3.80%*
3.3.1. Racks	$2,400	0.02%
3.3.2. Workstations and peripherals	$61,200	0.44%
3.3.3. Network equipment and COTS	$60,000	0.43%
3.3.4. Security equipment and COTS	$120,000	0.87%
3.3.5. Other COTS SW (Database management, Backup, Antivirus, OS for workstations, Analytics and reporting, etc.)	$90,000	0.65%
3.3.6. One Time password	$120,000	0.87%
3.3.7. Helpdesk hardware	$24,000	0.17%
3.3.8. HSMs	$48,000	0.35%
3.4. Team Vehicles	*$468,000*	*3.39%*
3.4.1. Vehicle (truck, car, motorbike, bike, etc.)	$360,000	2.61%
3.4.2. Vehicle running costs	$108,000	0.78%
3.5. Registrar's Full Kit	*$56,940*	*0.41%*
3.5.1. Laptop with camera	$15,600	0.11%
3.5.2. Backdrop (for picture quality)	$2,340	0.02%
3.5.3. Light system (for picture quality)	$2,340	0.02%
3.5.4. Fingerprint scanner	$12,480	0.09%
3.5.5. Iris capture	$9,360	0.07%
3.5.6. 2nd screen	$3,900	0.03%
3.5.7. Protection case	$3,120	0.02%
3.5.8. Bag	$780	0.01%
3.5.9. UPS	$4,680	0.03%
3.5.10. Printer (for enrolment receipt)	$2,340	0.02%
3.6. Registrar's Basic Kit (alternative to full kit)	*$41,340*	*0.30%*
3.6.1. Tablet with integrated fingerprint captor	$18,720	0.14%
3.6.2. Iris capture	$9,360	0.07%

ITEM	AMOUNT	%
3.6.3. Bag	$780	0.01%
3.6.4. Backdrop	$2,340	0.02%
3.6.5. Light system	$2,340	0.02%
3.6.6. UPS	$4,680	0.03%
3.6.7. Protection case	$3,120	0.02%
3.7. Mobile connectivity device (price for 4 years)	*$56,160*	*0.41%*
3.8. Robust Credential (With procurement and markups)	*$1,596,123*	*11.55%*
3.8.1. PVC card	$245,557	1.78%
3.8.2. Security feature (pre-personalized)	$613,894	4.44%
3.8.3. QR Code	$122,779	0.89%
3.8.4. Personalization cost (HW + SW + maintenance)	$368,336	2.67%
3.8.5. Consumable for card personalization	$122,779	0.89%
3.8.6. Card delivery cost	$122,779	0.89%
3.9. Authentication (with procurement & markup)	*$34,800*	*0.25%*
3.9.1. Scanner single fingerprint	$6,000	0.04%
3.9.2. Tablet with fingerprint scanner	$28,800	0.21%
3.10. Backup Hardware and Disaster Recovery	*$436,133*	*3.16%*
3.10.1. Hardware backup - in % of total HW	$73,253	0.53%
3.10.2. Disaster recovery site (no cost for ABIS licensing)	$362,880	2.63%
TOTAL	**$13,814,201**	**100.00%**