Procurement of Consultancy Services as Systems Integrator for the Supply, Delivery, Installation, and Maintenance of the Philippine Identification System (PhilSys)

Government of the Republic of the Philippines

PHILIPPINE STATISTICS AUTHORITY

Quezon City, Philippines

PUBLIC BIDDING NO. 2020-03

May 2020

Volume 2: Technical Specifications

Fifth Edition

October 2016

Table of Contents

List of Figures

List of Tables

Abbreviations

Table 1. Abbreviations

Abbreviation	Description
ABAS	Automated Biometric Authentication System
ABIS	Automated Biometric Identification Systems
AGC	Architecture Governance Committee
AMC	Annual Maintenance Cost
AMS	Authentication Management System
API	Application Programming Interface
APIMS	API Management System
ASEAN	Association of Southeast Asian Nations
ASR	Attack Surface Reduction
AV	Antivirus
BI	Bureau of Immigration
BIAS	Business Intelligence and Analytics System
BioSP	Biometric Service Provider
BPM	Business Process Management
BSP	Bangko Sentral ng Pilipinas
CBU	Card Batching Utility
CEPH	Free Storage Software Platform
CERT	Computer Emergency Response Team
CI/CD	Continuous Integration / Continuous Delivery
CIA	Confidentiality, Integrity and Availability
CICC	Cybercrime Investigation and Coordination Center
CII	Critical Information Infrastructure
CMC	Change Management Committee
CMS	Card Management System
CNCF	Cloud Native Computing Foundation

Abbreviation	Description
COTS	Commercial off-the-shelf
CPMS	Card Personalization Management System
CPS	Card Production System
CPU	Central Processing Unit
CRMS	Customer Relationship Management System
CRVS	Civil Registration and Vital Statistics
CSRF	Cross-Site Request Forgery
CSS	Cascading Style Sheets
CWE	Central Workflow Engine
DAMS	Database Activity Monitoring Solution
DBA	Database Administrator
DBM	Department of Budget and Management
DC	Data Center
DDoS	Distributed Denial of Service
DFA	Department of Foreign Affairs
DHCP	Dynamic Host Configuration Protocol
DICT	Department of Information and Communications Technology
DILG	Department of Interior and Local Government
DIMM	Dual Inline Memory Module
DLP	Data Loss Prevention
DMS	Document Management System
DMZ	Demilitarized Zone
DND	Do Not Disturb
DNS	Domain Name Server
DR	Disaster Recovery
DSWD	Department of Social Welfare and Development
e-GMP	E-Government Master Plan

Abbreviation	Description
eKYC	Electronic Know-Your-Customer
EMS	Enterprise Management System
ESB	Enterprise Service Bus
FDMS	Fraud Detection and Management System
FRC	Fixed Registration Centers
FRS	Functional Requirement Specifications
GC	Garbage Collection
GOCC	Government Owned & Controlled Corporation
GPS	Global Positioning System
GRC	Governance, Risk and Compliance
GSIS	Government Service Insurance System
GUI	Graphics User Interface
HA	High-Availability
HD	High Definition
HIPS	Host Intrusion Prevention System
HSM	Hardware Security Module
HTML	Hypertext Markup language
IAMS	Identity and Access Management System
ICT	Information and Communications Technology
ID	Identity / Identification
IDMS	Identity Management System
IIIT	International Institute of Information Technology
IMAC	Install, Move, Add, Change
IOPS	Input/output Operations Per Second
IPR	Intellectual Property Rights
ISO	International Organization for Standardization
ISSC	Information Security Steering Committee

Abbreviation	Description
IT	Information Technology
IVR	Interactive Voice Response
JDBC	Java Database Connectivity
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
KMS	Knowledge Management System
KYC	Know-Your-Customer
LCRO	Local Civil Registry Office
LMS	Learning Management System
MAS	Manual Adjudication System
MOA	Memorandum of Agreement
MOSIP	Modular Open Source Identity Platform
MPLS	Multiprotocol Label Switching
MVS	Manual Verification System
MZ	Militarized Zone
NBI	National Bureau of Investigation
NCSP	National Cybersecurity Plan
NEDA	National Economic and Development Authority
NIPS	Network Intrusion Prevention System
NOC	Network Operation Center
NPC	National Privacy Commission
NS	Notification System
NSFI	National Strategy for Financial Inclusion
NTP	Notice to Proceed
OCI	Open Container Initiative
OEM	Original Equipment Manufacturer
OS	Operating System

Abbreviation	Description
OTP	One-Time Password
OTS	Off-the-Shelf
OWASP	Open Web Application Security Project
PACS	Post and Courier System
PBD	Philippine Bidding Documents
PCN	PhilSys Card Number
PCOO	Presidential Communications Operations Office
PDMS	Partner and Device Management System
PFRC	PhilSys Fixed Registration Center
PhilSys	Philippine Identification System
PII	Personally Identifiable Information
PISA	PhilSys Information System Architecture
PKI	Public Key Infrastructure
PLDT	Philippine Long Distance Telephone Company
PMA	PhilSys Mobile Application
PMC	Project Management Committee
PNP	Philippine National Police
POS	Point of Sale
PRO-RSMS	PhilSys Registry Office – Registration and Systems Management Service
PSA	Philippine Statistics Authority
PSN	PhilSys Number
PSN-ASIF	PSN - Authentication Services Implementation Framework
PSNGTMS	PSN Generation and Tokenization Management System
PSPCC	PhilSys Policy and Coordination Council
PWP	PhilSys Web Portal
QA	Quality Assurance
QR	Quick Response

Abbreviation	Description
RAID	Redundant Array of Inexpensive Disks
RAM	Random-Access Memory
RFID	Radio Frequency Identification
RFP	Request for Proposal
RP	Relying Parties
RPAS	Relying Party Authentication System
RPO	Recovery Point Objective
RPS	Relying Parties Software
RTO	Recovery Time Objective
SAML	Security Assertion Markup Language
SATA	Serial Advanced Technology Attachment
SDK	Software Development Kit
SDLC	Software Development Lifecycle
SDS	Software Defined Storage
SEDA	State Event Driven Architecture
SFTP	Secure File Transfer Protocol
SI	Systems Integrator
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SOA	Service Oriented Architecture
SOAR	Security Orchestration, Automation and Response
SOC	Security Operation Center
SQL	Structured Query language
SRS	Software Requirement Specification
SSD	Solid-State Drive

Abbreviation	Description
SSS	Social Security System
SWS	Social Weather Station (a Philippine social research institution)
TB	Terabyte
TCO	Total Cost of Ownership
TRAIN	Tax Reform for Acceleration and Inclusion
TRN	Transaction Reference Number
TSPAS	Trusted Service Provider Authentication System
TSPS	Trusted Service Provider Software
UAT	User Acceptance Testing
UBA	User Behavior Analytics
UPS	Uninterrupted Power Supply
UTF	Unicode Transformation Format
VAPT	Vulnerability Assessment and Penetration Testing
VDI	Virtual Desktop Infrastructure
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XML	Extensible Markup Language
XSS	Cross-Site Scripting

1 Introduction

1.1 Purpose of this Terms of Reference

Bidders are invited to submit Proposal Information and Cost Quotations to the PSA for the Procurement of Consultancy Services as Systems Integrator for the Supply, Delivery, Installation, and Maintenance of the Philippine Identification System (PhilSys). Proposals should set forth an automated solution to the specific applications listed herein, identify and provide the operating environment, hardware, and software needed to run the systems, describe an implementation approach and timeline, and recommend an appropriate approach to training and implementation services.

The PSA is committed to selecting a Bidder for a 5-year contract from the issuance of Notice to Proceed (NTP) and conducting this procurement in an open and competitive manner in full compliance with appropriate regulations and policies.

1.2 Background

About the Philippine Identification System

Republic Act No. 11055 (the "Philippine Identification System Act"), signed into law in August 2018, established the Philippine Identification System (or PhilSys) as a foundational identification system for all citizens and resident aliens of the Republic of the Philippines. The declared policies of R.A. 11055 are to:

1. promote seamless delivery of service;
2. improve the efficiency, transparency, and targeted delivery of public and social services;
3. enhance administrative governance;
4. reduce corruption and curtail bureaucratic red tape;
5. avert fraudulent transactions and misinterpretations;
6. strengthen financial inclusion; and
7. promote ease of doing business.

Furthermore, the declared policies place importance on the deployment of a resilient digital system to secure the data collected and that the people's right to privacy, confidentiality and other basic rights are at all times upheld and protected.

The Government of the Republic of the Philippines in October 2018 and March 2019, respectively approved implementation rules and regulations (IRRs) for R.A. 11055 and a 5-year PhilSys Implementation Plan.

1.2.1 Implementation and governance arrangements for the PhilSys

The Philippine Statistics Authority (PSA) is the primary implementing agency for R.A. 11055 and has the mandate for the overall planning, management, and administration of the PhilSys. The PhilSys Registry Office (PRO) was established in PSA to carry out these responsibilities, headed by a Deputy National Statistician (DNS) at the Assistant Secretary-level. This new responsibility builds on PSA and its predecessors' historic mandate for leading the Philippines' civil registration and vital statistics (CRVS) system and recognizes the critical link of the integrity and sustainability of PhilSys with the continuous registration of births, deaths, marriages and other vital events. The PSA will collaborate with LGUs, other government agencies and GOCCs to carry out registration and other PhilSys-related services such as data updates and credential distribution.

In accordance with R.A. 11055, the Department of Information and Communications Technology (DICT) is responsible for providing technical assistance to PSA for the implementation of the PhilSys.

The PhilSys Policy and Coordination Council (PSPCC) formulates policies and guidelines to ensure effective coordination and implementation of the PhilSys. The composition of the PSPCC is:

1. Secretary, National Economic and Development Authority (NEDA) as Chairperson;
2. National Statistician and Civil Registrar General, Philippine Statistics Authority (PSA) as Co-Chairperson;
3. Undersecretary, Department of Budget and Management (DBM) as Vice Chairperson;
4. Undersecretary, Department of Foreign Affairs (DFA) as member;
5. Undersecretary, Department of Information and Communications Technology (DICT) as member;
6. Undersecretary, Department of Finance (DOF) as member;
7. Undersecretary, Department of Social Welfare and Development (DSWD) as member;
8. Undersecretary, Department of the Interior and Local Government (DILG) as member;
9. Chairperson, National Privacy Commission (NPC) as member;
10. Deputy Governor, Bangko Sentral ng Pilipinas (BSP) as member;
11. President and General Manager, Government Service Insurance System (GSIS) as member;

12. President and Chief Executive Officer, Philippine Health Insurance Corporation (PhilHealth) as member;
13. President and Chief Executive Officer, Social Security System (SSS) as member; and
14. Postmaster General, Philippine Postal Corporation (PHLPost) as member.

1.2.2 Procurement of Main Components of the PhilSys

The main components of the PhilSys have been or will be procured separately, namely:

1. Supply, Delivery and Managed Services of 5,000 Registration Kits for the Philippine Identification System (PhilSys) (awarded in August 2019);
2. Supply, installation, support and maintenance of Automated Biometric Identification Systems (ABIS) for Philippine Identification System (PhilSys) (awarded in April 2020);
3. Consultancy Services as System Integrator for the Philippine Identification System (PhilSys) (this procurement); and
4. PhilID card production and personalization, to be procured by the Bangko Sentral ng Pilipinas (BSP).

1.3 Objectives of the PhilSys

As a foundational identification system, the objective of the PhilSys is to improve the lives of all citizens and residents of the Philippines by making access, delivery and administration of Government and private sector services easier, wider, cheaper, faster, more secure, and more responsive to people's needs. Towards this end, the design and implementation of the PhilSys will ensure that the people's right to privacy, confidentiality and other basic rights are at all times upheld and protected.

1.3.1 Roles

The PhilSys will have two roles:

1. Creating a unique and secure digital legal foundational identity for each registered person; and
2. Allowing that digital legal foundational identity to be controlled by the registered person (as data owner consistent with RA 10173) and reliably verified both in-person and online for both Government and private sector transactions.

By simplifying the PhilSys to these two basic but important roles, the intention of the Government of the Philippines is to build an interoperable foundational platform and public infrastructure that can reach scale more quickly and cost-efficiently, taking advantage of relevant emerging digital technologies and approaches to digital government, including secure distribution of data, interoperability of information

systems, and the 'once only' principle for data collection and use. Minimizing the data to be collected and managed by the PhilSys to core identity attributes is a deliberate measure to safeguard data protection and privacy.

1.3.2 Implications for Functional Identification Systems and Registries

The focus of the PhilSys, as a foundational identification platform, on the above-mentioned two roles and on interoperability and data minimization allows relying parties and operators of functional identification systems and registries to have the flexibility to build and manage their applications (e.g. for authorization) on top of the PhilSys. For example, Government agencies responsible for delivering social assistance should be able to depend on the PhilSys for establishing the uniqueness of beneficiaries and for verifying the identity of beneficiaries when needed, and complementing this in their own information systems with data that are relevant for their functions (e.g. targeting of beneficiaries and administration of benefits).

To reduce duplication, the PhilSys may replace existing functional identification systems and registries that exclusively serve the purposes of identification and verification.

There are functional identification systems and registries that do more than identification and verification (i.e. authorization) and therefore have specific uses (e.g. a driving license proves that a holder is eligible to drive, a passport facilitates travel across international borders for the holder, and the UMID is used for a variety of benefits including as a cash card for SSS and GSIS members), which will not be replaced by the PhilSys. However, these systems will have their integrity enhanced and costs reduced by basing their identity proofing and deduplication on the PhilSys (see illustration below). For example, new functional identification systems and registries should not need to collect biometrics to establish uniqueness of their customers because they can depend on the unique identity created by the PhilSys for this purpose.

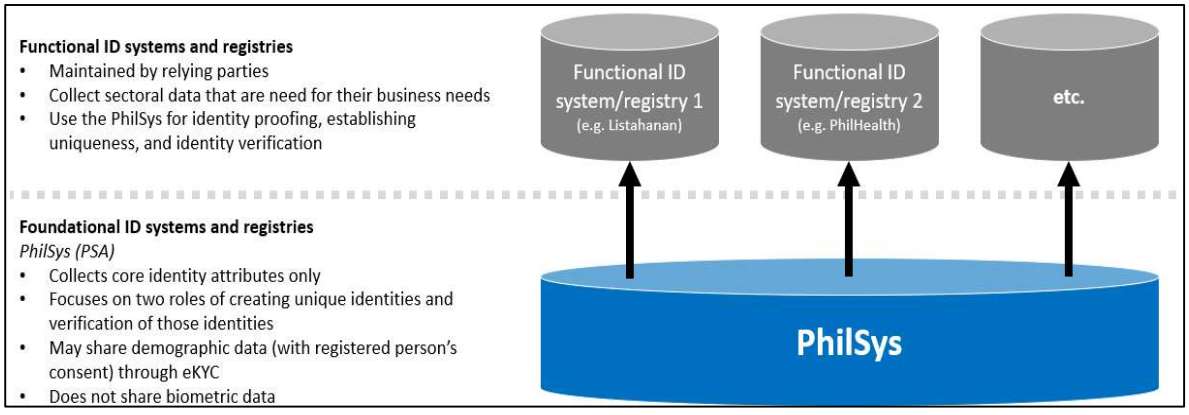

Figure 1. Relationship between the PhilSys and Functional Identification Systems

1.4 Principles

The PhilSys will adopt and create international best practices in terms of inclusion, design, technology neutrality, performance, interoperability, cost-efficiency, data protection, privacy, and cybersecurity. In doing so, the PhilSys will observe the Principles on Identification for Sustainable Development as a guiding framework for maximizing its developmental impact while mitigating risks (see box below).

Principles on Identification for Sustainable Development[1]

Inclusion: Universal coverage and accessibility

1. Ensuring universal coverage for individuals from birth to death, free from discrimination.
2. Removing barriers to access and usage and disparities in the availability of information and technology.

Design: Robust, secure, responsive and sustainable

3. Establishing a robust—unique, secure, and accurate—identity.
4. Creating a platform that is interoperable and responsive to the needs of various users.
5. Using open standards and ensuring vendor and technology neutrality.
6. Protecting user privacy and control through system design.
7. Planning for financial and operational sustainability without compromising accessibility.

Governance: Building trust by protecting privacy and user rights

8. Safeguarding data privacy, security, and user rights through a comprehensive legal and regulatory framework.
9. Establishing clear institutional mandates and accountability.
10. Enforcing legal and trust frameworks through independent oversight and adjudication of grievances.

[1.] The Principles on Identification for Sustainable Development have been endorsed by 25 international, regional academic and private sector organizations. For more information, visit id4d.worldbank.org/principles

1.5 Envisaged Benefits

The PhilSys will transform the Government and private sectors in the Philippines by making their public services more inclusive and more digital. It will achieve this by digitalizing and automating the identification and verification of Filipinos and resident aliens, which are fundamental processes in accessing, delivery and administering all services that involve interacting with people.

The PhilSys will accelerate achievement of *AmBisyon Natin* 2040, the Philippines' long-term development vision, and the medium-term Philippine Development Plan (2017-2022) – and, in particular, its objectives of *Malasakit* (fostering trust in public institutions and among Filipinos), *Pagbabago* (inequality-reducing transformation) and *Patuloy na Pag-unlad* (increasing potential growth). It will also support implementation of priority initiatives of the Government of the Philippines

including the economic recovery plan in response to the COVID-19 pandemic, the Tax Reform for Acceleration and Inclusion (TRAIN) agenda, the Universal Healthcare Coverage Act, the National Strategy for Financial Inclusion (NSFI), the modernization of social protection and social security, the E-Government Master Plan (e-GMP), and efforts to strengthen the resilience and response of the Philippines to natural calamities. In doing so, the PhilSys will also contribute to achieving the Sustainable Development Goals (SDGs), including targets related to ending poverty, universal health coverage, financial inclusion, and providing legal identity for all, among others.

The benefits of the PhilSys can be summarized as follows:

1. **Making services more accessible**: Because the PhilSys will itself be accessible to all Filipinos and resident aliens (through inclusive registration requirements) and its credentials will be accepted by themselves for most transactions, it will democratize access to financial, social welfare and security, health, education, and other Government services. This will be especially beneficial for remote and far-flung areas where using technology, the PhilSys will reduce the costs for service providers and make it easier for service providers to offer more services either through the internet or using agents with equipment that can leverage the PhilSys, without depending on brick-and-mortar offices, such as banking and e-money agents.

2. **Promoting ease of doing business**: Because the PhilSys will provide a platform for Government and private sector service providers to identify and verify their customers in a digital and automated manner for both in-person and online transactions, it will reduce the paper-work, red-tape, and bureaucracy required for processes that are currently often done manually, and therefore reduce administrative costs, time and risks. This will be especially beneficial for local and central Government services that are partially or completely made to be available through online channels (e.g. various registrations, renewals and permits).

3. **Enhancing the integrity of services and reducing fraud**: Because the PhilSys will uniquely identify each registered person at a national scale and allow that identity to be verified with a high level of assurance, it will help eliminate instances of identity fraud (e.g. impersonation, identity theft and 'ghosts') and strengthen the integrity of functional identification systems and registries. This will be especially beneficial in social assistance and social security programs, where the PhilSys will contribute to ensuring that the right beneficiaries are receiving benefits (e.g. through verification and by linking the PSN to a beneficiary's bank or e-money account) and by making it easier for them to open bank and e-money accounts to receive cash transfers digitally, and the financial sector, where the PhilSys will contribute to financial integrity, addressing money-laundering risks and better credit history data.

4. **Enabling and promoting participation and trust in digital government and the digital economy**: Because the PhilSys will digitalize underlying processes for service access, delivery, and administration and enable the verification of identity over the internet with a high level of assurance (i.e. without the need for a face-to-face transaction), the PhilSys should enable a broader transition to digital, online citizen-centric service delivery by Government and the private sector, as well as create opportunities innovation and new products and services. This

will be especially beneficial for allowing Government departments and agencies to exchange data, when consented or warranted, to improve the effectiveness and efficiency of their programs.

5. **Empowering Filipinos and resident aliens with greater control over their personal data**: Because the PhilSys will give PSN-holders the ability to determine who can see and what data can be shared about them when carrying out transactions using the PhilSys, it will contribute to greater transparency and accountability for how data is used in the Philippines. Furthermore, the PhilSys will allow PSN-holders to 'hide' their permanent PSN through the use of a PhilSys Card Number (PCN) (as the ID number printed on the PhilID card), *Alyas* PSN (as an ID number for specific transactions), and PSN tokens (as the ID number stored by functional ID systems and registries). Aside from promoting data protection, this will be especially beneficial as the Philippines' digital economy grows and new products and services making use of data emerge.

6. **Facilitating cross-border transactions**: There is an opportunity for PhilSys credentials to be recognized in other jurisdictions, which could facilitate migration, economic integration and trade, especially in relation to the digital economy. This will be especially beneficial for boosting the Philippines' international economic competitiveness and in the context of the ASEAN Economic Community.

1.6 Indicative Use Cases

Refer to Annex A – Use Cases for PhilSys

1.7 Stakeholders

Table 2. Stakeholders Description

Actor	Role
Filipinos and resident aliens	Participate in and benefit from the PhilSys through registration, verification at service access, updating their data, and reporting complaints.
Relying Parties	Provide Authentication Service using PhilSys to uniquely identify and verify the identity of their customers, in accordance with relevant laws, regulations, and guidelines. These are public and private sector service providers that are on-boarded into the PhilSys. Examples: Government agencies and GOCCs; Financial service providers; Mobile network operators; E-commerce websites.
Philippine Statistics Authority (PSA)	Lead implementing entity of the PhilSys including development, communication, provision of authentication services, overall coordination, data processing and management, and complaint management. Implementation of the PhilSys will be spearheaded specifically by the PhilSys Registry Office, headed by a Deputy National Statistician (Assistant Secretary-level).
Bangko Sentral ng Pilipinas (BSP)	Procurement and pre-personalization of the PhilID cards and providing physical space and equipment for PSA staff to handle the personalization process.
PhilSys Policy and Coordination Council (PSPCC)	Formulating policies and guidelines to ensure effective coordination and implementation of the PhilSys, and ensuring compatibility of the respective technology infrastructure of different government agencies in order to comply with the requirements of PhilSys.
National Economic and Development Authority (NEDA)	Chairs the PSPCC and represents PSA for budget purposes and in the Cabinet.
Department of Information and Communications Technology (DICT)	Provides technical assistance to the PhilSys and shared government ICT including data center space and hosting, and WAN connections.
National Privacy Commission (NPC)	Ensuring compliance with the Data Privacy Act and providing technical assistance related to data protection and privacy.

Actor	Role
Department of Budget and Management (DBM)	Approving and monitoring the budget and plantilla of the PhilSys Registry Office.
Department of Foreign Affairs (DFA)	Providing physical space and staff at overseas missions to deliver PhilSys services to overseas Filipinos, including registration, credential distribution, data updates, and grievance handling.
Bureau of Immigration (BI)	Facilitating the registration of resident aliens.
Presidential Communications Operations Office (PCOO)	Implementation of the PhilSys communications strategy.
Civil society	Facilitate effective communications and outreach, particularly to marginalized and vulnerable population groups, and working with the Government to improve the design and implementation of the PhilSys.
Media	Facilitate effective communications and outreach, particularly to marginalized and vulnerable population groups.

1.8 Key Features of the PhilSys

1. **Pre-Registration service:** Pre-registration allows Filipinos and resident aliens to provide through a secure website or application their demographic data in advance and to schedule an appointment at a PhilSys Fixed Registration or Mobile Registration Center for validation of the demographic data and capture of biometrics to complete the registration cycle. An appointment reference number is issued to acknowledge submission of the demographic data and to retrieve it when the applicant visits a registration center. The intention of pre-registration is to make the process convenient for applicants and to speed up data capture at registration centers, which will allow the PhilSys to register more people per day.
2. **Registration service:** Registration involves Filipinos and resident aliens providing the prescribed demographic and biometric data to a registration officer using a registration kit at a PhilSys Fixed Registration or Mobile Registration Center, in order to be included in the PhilSys and to be allotted a PSN and other credentials. Applicants who have pre-registered can provide their pre-registration reference number to retrieve their demographic data from their earlier submission. The process involves validating the demographic data provided against supporting evidence (e.g. IDs or an introducer) on the front-end (i.e. by a registration officer) and deduplication of the applicant against the records of registered persons on the back-end. Supporting evidence is scanned and recorded for audit purposes, and may be subject to cross-referencing against source data (e.g. passport records at DFA). A transaction number and slip for the registration is provided to the applicant so they can track the status. Registration service details are provided in Section 6.2.1 of this document.
3. **PSN generation and tokenization services:** PSN generation involves the allotment of a unique 12-digit PSN to a registered person after they have successfully completed the registration process by being found to have provided correct data and have not registered before. Tokenization is a deliberate data protection strategy to safeguard the privacy of registered persons and the security of the PSN. It involves the generation of derivatives of the PSN to be used by registered persons and registered relying parties in lieu of a PSN for any purposes (e.g. authentication, seeding or data sharing and interoperability) in order to enable registered persons to conceal the PSN as a permanent, irrevocable and unique identifier. See Section 1.13 on Credentials for more information.
4. **Authentication and eKYC services:** Authentication involves a registered relying party verifying the identity of a registered person against the registered person's PhilSys record. eKYC involves the transmission of the minimum demographic data needed back to the registered relying party, only following a successful online authentication. Eventually, most online authentications will be processed through a Trusted Service Provider (TSP), which is an intermediary between registered relying parties and the PhilSys Information System. See Section 1.14 on Methods of Authentication for more information.
5. **Lifecycle data updates:** Lifecycle data updates involves registered persons updating their name, mobile number, address, and email either online through the PhilSys Portal / PhilSys Mobile Application or in assisted mode in the Fixed Registration Centers. Evidence to support changes (e.g. of names) will be defined by guidelines developed by the PSA. This service would also

allow children at the age of 5 and 15 years to update their biometric information. In case of loss of PSN or PhilID, this service would define methods of recovery.

1.9 Eligibility for Registration

The PhilSys is accessible to all Filipino citizens inside and outside of the Philippines as well as resident aliens, defined as non-citizens who have established residency in the Philippines for a period of more than 180 days. The PhilSys will cover all age groups.

1.10 Data Collected

Pursuant to R.A. 11055, the following data will be collected in the PhilSys and kept in each registered person's record:

1. Demographic data (collected at all ages):
    a. Full name (mandatory)
    b. Sex (mandatory)
    c. Date of birth (mandatory)
    d. Filipino or Resident Alien (mandatory)
    e. Blood type (mandatory, subject to exceptions)
    f. Permanent address (mandatory)
    g. Present address (optional)
    h. Mobile number (optional)
    i. Email address (optional)
    j. Marital status (optional)
2. Biometric data (captured at age 5 and recaptured at age 15):
    a. Facial image (mandatory, subject to exceptions)
    b. Ten (10) fingerprints (mandatory, subject to exceptions)
    c. Two (2) iris scans (mandatory, subject to exceptions)
    d. If necessary, other identifiable features of an individual as may be determined in the IRR
3. Record history / Metadata (for all ages):
    a. Place of registration (mandatory)
    b. Date and time of registration (mandatory)
    c. Registration operator (mandatory)

d. Scan of the registration form (mandatory)

e. Scan of supporting documentation for registration (mandatory)

f. Modifications made to the record (mandatory)

g. Date and time of modifications (mandatory)

h. Scan of application form for modifications (mandatory)

i. Scan of supporting documentation for modifications (mandatory)

j. Date and reasons of issuance, re-issuance and cancellation of the PhilID

k. Reasons for the omission of any mandatory data (mandatory)

l. Details of authentication requests, including the date, requesting entity and response provided by the PhilSys (mandatory, the period of retention defined by the registered person)

m. Disclosure, conveyance, dissemination, publication, and use of information by third parties (mandatory)

n. Other relevant information regarding the registration, modification, and authentication of personal information of a registered person under R.A. 11055

1.11 Registration Channels and Processes

The PSA will offer registration and other PhilSys related services to Filipino citizens inside the Philippines and resident aliens by establishing: (a) fixed registration centers, such as in premises of Government agencies and GOCCs (e.g. PSA Regional and Provincial Offices, LCROs, and branches of PhilHealth, PHLPost, SSS and GSIS); and (b) mobile registration centers in public spaces, in coordination with LGUs and other stakeholders. The PSA will provide software, hardware, staff, and will set standards on the physical environment of fixed and mobile registration centers. The terms of the use of premises and public spaces will be negotiated with each partner through a Memorandum of Agreement (MOA).

The PSA will coordinate with the Department of Foreign Affairs (DFA) to offer registration and other PhilSys related services to overseas Filipino citizens at overseas Philippine missions. The PSA will provide all necessary software and hardware and will set standards on the physical environment. DFA staff will be trained by PSA to carry out registration and other PhilSys related services.

1.12 Collaboration with Civil Registration

In line with best practices on the harmonization of civil registration and identification services, the PhilSys will collaborate with the Civil Registration Service to authenticate vital events such as births, deaths and marriages, in order to coordinate up-to-date authentic information with use case relying parties in compliance with existing laws, rules and regulations.

1.13 Credentials

The random 12-digit PhilSys Number (PSN) is the primary PhilSys credential for each registered person. A PSN is unique to every registered person and every registered person is assigned only one PSN. The IRRs for R.A. 11055 set out conditions for the deactivation and reactivation of a PSN.

To strengthen the privacy of the registered person and the security of the PSN as a permanent, irrevocable and unique identifier – as well as to give registered persons better control over their identity data – the permanent PSN itself should not be used for authentications/eKYC transactions, should not be stored by relying parties nor used for sharing data between relying parties, and is not printed on the PhilID card (e.g. like a bank account number is not printed on a debit card). Instead, the PhilSys will use tokenization to generate tokens (as derivatives of the PSN) that can be used in lieu of the permanent PSN in different circumstances to achieve three different outcomes: (1) to allow a registered person to verify their identity; (2) to allow relying parties to establish uniqueness of an individual within their own context; and (3) to allow relying parties to share or verify data on the same registered person, when legally authorized (e.g. through consent).

The types of PSN tokens (all linked to a registered person's PSN) are as follows:

1. **PhilSys Card Number (PCN)**: A 16-digit random unique number printed on the face of the PhilID card that is valid for the period that the PhilID is valid (i.e. until the card is replaced or reported as lost or stolen).

2. ***Alyas* PSN**: A 16-digit random unique number that is generated by the PhilSys at the registered person's request, in order to facilitate a verification. Multiple Alyas PSNs can be active at the same time for a registered person.

3. **Tokens for 'seeding' and data sharing by relying parties:** The SI will propose innovative techniques for the PhilSys to use tokenization to allow: (i) individual relying parties to establish the uniqueness within their context of a registered person without needing to collect and store the PSN, PCN or Alyas PSN (i.e. a stable identifier or token that is unique for a registered person for a relying party – such as a back-end token); and (ii) two or more relying parties to share or verify data on the same registered person, without the need to match a PSN, PCN or Alyas PSN (such as a correlation token).

4. The secondary PhilSys credentials are the:

5. **PhilID card**: A simple plastic card with overt security features used primarily as a physical medium to convey the PCN, registered demographic data and facial image, and a digitally-signed Quick Response (QR) code encoded with demographic data, and two best fingerprints' labels. Rather than incorporate expensive covert or forensic physical security features, the PhilID card will primarily draw its security from online authentication through the PhilSys.

1.14 Methods of Authentication

The following methods of authentication of registered persons will be offered by the PhilSys:

Offline

1. **PhilID taken at face value**: For low-risk transactions, the relying party will review the PhilID card and compare the information (e.g. the facial image) with that of the bearer as well as examine the quality and overt security features of the PhilID card.

Online

2. **Fingerprint, iris or facial image biometric authentication**: a registered relying party collects a PSN, PCN or Alyas PSN and an image of a fingerprint, iris and / or face of a registered person claiming an identity. This data is transmitted through a secure connection to the PhilSys, templated and compared with templates of the same biometric(s) in the record of the corresponding PSN. Eventually, most of these transactions will be processed through a Trusted Service Provider (TSP) that will be an intermediary between registered relying parties and the PhilSys Information System. Based on the matching threshold, only a positive or negative response is returned to the relying party.

3. **Demographic authentication**: a registered relying party collects a PSN, PCN or Alyas PSN and demographic information such as name, date of birth, sex, etc. or other PhilSys demographic data of registered persons claiming an identity. This data is transmitted through a Trusted Service Provider (TSP) over a secured connection to the PhilSys, and compared with the data stored of the corresponding PSN in the PhilSys Registry. Only a positive or negative response is returned to the relying party.

4. **One Time Password (OTP) by SMS**: A registered relying party collects a permanent PSN, PCN or Alyas PSN of a registered person claiming and this data is transmitted through a secure connection to the PhilSys for the PhilSys to send a temporary 6-digit number by SMS to the mobile number in the record of the corresponding PSN. The person claiming the identity should provide the 6-digit code to the relying party, which is transmitted through a secure connection to the PhilSys to match against the 6-digit code it sent. A positive or negative response is returned to the relying party.

5. **Electronic Know Your Customer (eKYC)**: Only in circumstances enabled by law and consented by the registered person (e.g. customer due diligence regulations in the financial sector or applying for a passport or social benefit), the relying party may receive through secure transmission specific demographic data and the facial image from the PhilSys following a successful biometric and / or OTP authentication.

1.15 Data Protection, Privacy, and Cybersecurity

The security and integrity of Personally Identifiable Information (PII) in the PhilSys is the highest priority. Therefore, the design and implementation of the PhilSys will emphasize data protection, cybersecurity and the privacy of the registered persons whose data it holds. Furthermore, the PhilSys will give registered persons – as data subjects – ultimate control over their personal data.

These outcomes will be achieved through a dual "privacy- and security-by-design" approach of strict compliance with legal safeguards provided for by the Data Privacy Act and the Philippine Identification System Act, and adoption of cutting-edge privacy-enhancing technologies.

Key data protection and privacy features and principles of the PhilSys in this context include:

1. Minimal data collection.
2. Focusing on verifying the identity of registered persons through a binary "yes / no" approach rather than sharing data.
3. Only disclosing demographic data to relying parties when consented and required by law and only the specific data that is consented and needed by law, including never sharing biometric data with any third party.
4. Enabling tokenization of the permanent PSN, including the PCN, Alyas PSN, and other tokens for seeding and data sharing by relying parties.
5. Strict access controls, encryption, and security of data at times of capture, transmission and storage.
6. Providing a self-service portal, available online and at PhilSys Fixed Registration Centers, to allow registered persons to see who has accessed their data, when and why, to lock / unlock their record for authentications, to update certain data attributes (e.g. residential address), and to define the period that authentication transaction logs will be retained.
7. Tamper-proof logging of transactions for auditing and traceability purposes.
8. Regular security audits of PhilSys software, hardware, and processes.
9. Making freely and easily available grievance mechanisms.

Furthermore, with respect to cybersecurity, the PhilSys is defined as a Critical Information Infrastructure (CII) within the framework of the Philippines' National Cybersecurity Plan (NCSP) 2022. The PhilSys will be designed and implemented in alignment with the NCSP 2022. In doing so, the PSA

will work closely with the DICT, Cybercrime Investigation and Coordination Center (CICC), National Bureau of Investigation (NBI), Philippine National Police (PNP) and the intelligence community to identify, protect, detect, respond and recover against any domestic and foreign threats to the PhilSys cybersecurity, including risk management. As part of this, the PSA will establish its own Computer Emergency Response Team (CERT), which will coordinate with the National CERT.

1.16 Interoperability and Technology Neutrality

The Government of the Philippines is committed to building the PhilSys as an interoperable platform that is fully owned and operated by the Government. Technology neutrality is important for making components of the PhilSys exchangeable and upgradeable when the need arises.

As part of this, the PhilSys will adopt international open standards and open source software (where appropriate), and ensure that procurement and contract management will reduce risks of technology and vendor lock-in or dependency.

2 PhilSys Information System Architecture

To facilitate the development, commissioning, and implementation of the PhilSys Information System, PSA adopted the PhilSys Information System Architecture (PISA) as its reference system architecture shown in the figure below. The PISA is governed by several principles of sustainable development[1] endorsed by various organizations and literature on global best practices for identification systems, Republic Act No. 11055 (the Philippine Identification System Act), Republic Act No. 10173 (the Data Privacy Act), their implementing rules and regulations (IRRs), and other relevant regulations and guidelines. Aligning PISA with these principles allows PSA to objectively assess that the proposed technology solutions are indeed responsive to the overall requirements of PhilSys.

The PISA has been designed in such a way that the upper layers have underlying technical dependencies from each of the layers below (see Figure 2). Conversely, the lower layers must be able to meet the demands and workloads defined by the upper architectural layers. The diagram also shows that all layers are incorporated into an encompassing information security design (which will be discussed in a separate Section 9 Information Security). Furthermore, the diagram illustrates that each of the architectural layers is abstracted (i.e. intentionally removing details and attributes at this stage). This approach gives more flexibility for the PSA and its chosen Systems Integrator (SI) to define various technical mappings, connectors, integration, and solutions that (i) cuts between various architectural components within the same layer and (ii) across architectural components from multiple layers.

The PISA has four (4) information system architectural layers, namely: Functional Architecture, Applications Architecture, Data Architecture, and Infrastructure Architecture. This document will further discuss each of the architectural layers in the succeeding sections.

[1] The Principles on Identification for Sustainable Development have been endorsed by 25 international, regional academic and private sector organizations. For more information, visit id4d.worldbank.org/principles

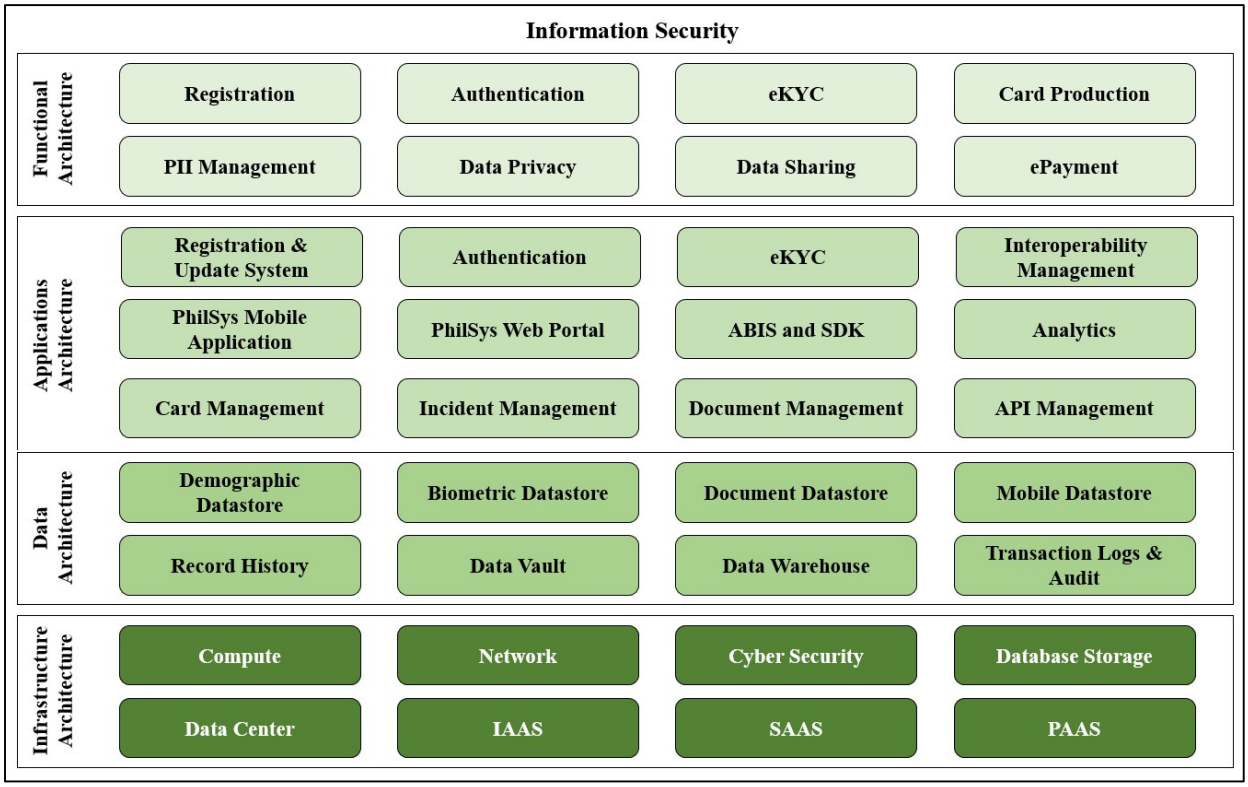

Figure 2. PhilSys Information System Architecture

2.1 Functional Architecture

Functional Architecture focuses on the operational requirements of the PhilSys Information System. Its components are:

1. **Registration** – Includes policies, guidelines, and procedures on registering individuals into the PhilSys Registry.
2. **Authentication** – Includes the policies, guidelines, and procedures on authenticating registered persons with the PhilSys Registry.
3. **eKYC** – Includes policies, guidelines, and procedures for onboarding customers to services by electronically transmitting customer data from the PhilSys Registry and only upon the registered person's successful authentication and consent.
4. **Card Production** – Includes policies, guidelines, and procedures that cover PhilID production and personalization.
5. **PII Management** – Includes policies, guidelines, and procedures adopted by PhilSys on managing the data subject's personally identifiable information.
6. **Data Privacy** – Includes policies, guidelines, and procedures on ensuring that data privacy is embedded in the design and implementation of the PhilSys Information System.

7. **Data Sharing** – Includes the policies, guidelines, and procedures applied to the data sharing, transmission from and to the PhilSys Information System.
8. **E-Payment** – Includes the policies, guidelines, and procedures that cover electronic payments.

2.2 Applications Architecture

The Applications Architecture focuses on the software solutions directly supporting the functional requirements. Its components are:

1. **Registration and Updates System** – An application that facilitates the entry of records to register a person into the PhilSys Registry. This component also includes the facility to update PhilSys Registry records of registered persons.
2. **Authentication** – An application that facilitates authentication of a registered person. This component compares the demographic or biometric characteristics of an individual against the PhilSys Registry and returns the authentication results to the relying party.
3. **eKYC** – This application facilitates eKYC authentication of a registered person. This component compares the demographic/biometric characteristics of an individual against the PhilSys Registry and returns the eKYC data to the relying party.
4. **PhilSys Web Portal** – This is primarily a web-based application that facilitates various requests and services needed by the applicant or registered person from the PhilSys Information System.
5. **PhilSys Mobile Application** – This is a mobile-based application that facilitates various requests and services needed by the applicant or registered person from the PhilSys Information System.
6. **ABIS & biometric SDKs** – Encompasses the software components that process biometric data within PhilSys.
7. **Interoperability Management** – This application leverages tokenization to enable secure data sharing between two or more on-boarded Relying Parties without having access to the permanent PSNs.
8. **Analytics** – Includes software components needed for monitoring and reporting on various parts of the PhilSys Information System.
9. **Card Management** – Covers the software components used for pre-personalization and personalization of the PhilID.
10. **Incident Management** – Refers to the software components used to detect, manage, and resolve incidents from various systems and parts of the PhilSys.
11. **Document Management** – Refers to the software solution for managing electronic and digitized documents needed by various systems and processes of PhilSys.

12. **API Management** – Refers to the software solution that abstracts the data access to and from various data stores identified in the Data Architecture Layer and software components in the Applications Architecture Layer.

2.3 Data Architecture

The Data Architecture focuses on the organization and management of data used by the software in the application layer. Its components are:

1. **Demographic Data Store** – Refers to both the logical and physical data store of demographic data and metadata of registered persons and applicants of PhilSys.
2. **Biometric Data Store** – Refers to both the logical and physical data store of biometric data and metadata of registered persons and applicants of PhilSys.
3. **Document Data Store** – Refers to both the logical and physical data store of document data and metadata of registered persons and applicants of PhilSys.
4. **Mobile Data Store** – Temporary logical and physical data store in registration kits and devices pending data upload to the central server.
5. **Record History** – Refers to both the logical and physical data store for data and metadata as prescribed by Section 5.i. of the Philippines Identification System (RA 11055).
6. **Data Vault** – Logical and physical data store that receives the unprocessed and unopened packets of data from registration kits and devices.
7. **Data Warehouse** – Refers to both the logical and physical data store built for analytical and reporting requirements of PhilSys.
8. **Transaction Logs and Audit** – Logical and physical data store that immutably records critical events and activities in the PhilSys Information System.

2.4 Infrastructure Architecture

The Infrastructure Architecture guides the deployment of hardware, equipment, and services supporting the needs of PhilSys architectural components. Its components are:

1. **Compute** – Includes solutions servers for processing requests and automation requirements.
2. **Network** – Includes solutions for linkage and routing of various physical components under the PhilSys network.
3. **Cyber Security** – Includes solutions for proactive monitoring, detection, and resolution of external and internal attacks against various PhilSys components.
4. **Database and Storage** – Includes solutions for highly available storage systems, databases, and services.

5. **Data Center** – Includes solutions and services provisioning for space, power, security, and connectivity for various physical computing, storage, network, and security assets of PhilSys.
6. **Infrastructure as a Service** – Includes integrated solutions for infrastructure requirements of PhilSys.
7. **Software as a Service** – Includes cloud-based solutions for application requirements of PhilSys.
8. **Platform as a Service** – Includes cloud-based solutions for platform requirements of PhilSys.

3 PhilSys Implementation Roadmap

The PhilSys implementation is governed mainly by the PSA registration strategy.

The table below shows the volume of registration by phase.

Table 3. Registration Roadmap

#	Stages of Registration	Volumes	Period
1	Pilot Registration	1 million	3Q 2019-June 2020
2	Phase-I Registrations of household heads	5 million	2020
3	Phase II Registrations	104 million	2021-2022

4 Demand Capacity

The tables below provide the details of registration workload and age analysis of the citizens and residents proposed to be registered in the PhilSys. The estimated population of the Philippines as per the census 2015 stands at 100.98 million. Whereas the estimated population by the year 2022 based on the current growth rate is projected to be 110 million. It is understood that children below the age of 5 years will be registered without biometric data capture. Hence, the net biometric registration is approximately 94 million. However, children upon reaching the age of 5 will be eligible for biometric registration. The estimated workload is shown in the tables below. The annual number of births is approximately 1.7 million, hence, on a base population of 94 million for biometric registration, it can be estimated that additional 1.7 million biometric registrations would be added to the base registration every year.

4.1 Estimated Registration Volumes

This section provides the details of the Registration volumes that will be covered in the various stages of Registration Roadmap provided in Section 3 above. A tabular representation of the estimated volumes in the overall project implementation is given below:

Table 4. Estimated Registration Volumes

Parameter	Description	Sizing Estimation
Current Population	Population in 2015 (a)	100.98 million (Source: Census 2015)
Estimated Population	Estimated Population in 2022 (b)	110 million
Population below 5 years	Estimated Population in 2022 (c)	16 million
Philippines Citizens outside the country	Estimated population (d)	10 million
Total Population for Biometric registration within the country by July - 2023	(e) = (b)-(c)-(d)	84 million
Population Growth rate (%)	Net growth rate (birth minus death)	1.72 %
Crude Birth Rate (%)	Number of Birth in 2018	1.52% per year
Crude Death Rate (%)	Number of Death in 2018	0.55% per year
Average No. of Births	The annual number of births in the period 2020-2030	1.7 million to 1.8 million per annum

Parameter	Description	Sizing Estimation
Average No. of Deaths	The annual number of deaths in the period 2020-2030	0.6 million per annum
Estimated registration of Citizens outside the Philippines	Annual %	20% of 10 million

4.2 Transaction Volumes

The estimates of registration volumes are given below. The overall registration target is 110 million registration of citizens and residents of the Philippines. However, some facts need to be paid special attention to while undertaking capacity planning. These are:

a. The count of the population below 5 years is approximately 16 million
b. The count of Overseas Filipinos is approximately 10 million
c. These citizens at (a) and (b) above shall come for Registration in a phased manner

Table 5. Estimated Transaction Volumes

Parameter	Description	Sizing Estimation
Pilot registration	Including biometric capture	1 million - start by 3Q 2019
Registration for de-duplication and PSN allotment	Estimate of registration records for deduplication	84 % population by 2022
Registration Target for de-duplication and PSN allotment	Entire Population of the Philippines	110 million, by end 2023 and beyond
Continuous registration of Children	Population comprising of 0-4 age group	15 % of the population of the base year of 2015 census age group 0-4
Continuous Registration of Citizens outside the Philippines	10% of the total population	20% of 10 % per annum
Existing PSN Deactivations	After PSN generation (due to deaths or loss of Filipino Citizenships)	Annual Death Rate of 0.6%
Biometric Updates	At 5 years	2.2 million per annum (population of 4-year-old children)

Parameter	Description	Sizing Estimation
Biometric Updates	At 15 years	2.2 million per annum (population of 14-year-old children)
Demographic Updates	Change in demographic details	5.5 million per annum (5% of Population)

The table given above is an estimate of the Registration and update volumes under this program. The detailed explanation of the line items is provided below:

a. Overall, the total population of the Philippines is considered at 110 million at the end of the year 2023. For the purpose of Registration of all the citizens and residents of the Philippines, it is estimated that 84% of the population will be registered. Thereafter, an additional 16% of the population will be covered 2023 onwards.

b. In addition to the Registration volumes as mentioned above, the continuous Registration of the annual increment in the population (new-born children) will be carried out. Moreover, the updates in demographic information such as mobile number, address, email address, etc. will also be carried out. Similarly, the update in biometric information will be carried out at the age of 5 years, 15 years and on-demand basis for other registered individuals.

4.3 Registration and Transaction Volumes

Table 6. Indicative Transaction Volumes

#	Parameter	Indicative Units
Registrations		
1.	Peak Registrations per day	Capacity 175,000 registration per day
2.	Peak Registration packet to be uploaded per day (incl. backlog)	At peak capacity 200,000 registrations per day
3.	Peak Registration batch process per hour (incl. backlog) for peak capacity	8,500 registration packets per hour
4.	Number of Concurrent internet users	2,500
5.	Average no. of hits by same users during the same login on the web page	2
6.	Web-users during peak hour	~100,000

#	Parameter	Indicative Units
7.	Web-users during peak hour	• 2.5% users / day • Peak hour will see double of average requests
Miscellaneous		
8.	Assumed CPU and memory Utilization for Non-ABIS Application	60%
9.	Bandwidth at each Fixed Registration Center to be provided by PSA or its nominated agency	4 Mbps
10.	Number of authentication requests (At peak load)	5 million per day
11.	Number of eKYC requests (At peak load)	2 million per day

4.4 Data Size

This section provides the details of the data size required to be handled in the PhilSys Information system.

Table 7. Data Size

Parameter	Description	Sizing Estimations
Size of Registration Packet	Demographic, 1 portrait photo, 2 Iris, 10 fingers and scanned documents	5 MB Raw Packet
Authentication Packet	Demographic, OTP, Iris or Facial	5 KB
eKYC Packet	OTP, Iris or Facial	30 KB

4.5 Estimation of PhilSys users

Table 8. Estimation of Users

Parameter	Description	Sizing Estimations
Total User	Total Number of Operators	5500 Registration Kit Users
Kit Operators	Field Operators	5000
	Supervisors	250 supervisors for PFRCs; 1 supervisor for each team of PFRC

Parameter	Description	Sizing Estimations
	Fixed Operators	250
	Working Hours	8 hours x 22 working days per month
Verification	Document Screener	500 Screeners (Minimum of 2 per PFRC)
	Working Hours	8 hours x 22 working days per month
Manual Adjudicators	Manual Adjudication	10 per shift
	Working Hours	8 hours per shift x 2 Shift
Manual Verification	Manual Verification	10 per shift
	Working Hours	8 hours per shift x 2 Shift
IT Helpdesk (indicative – operated by the SI)	Helpdesk Personnel	5 (First Shift) + 5 (Second Shift) + 3 (Third Shift)
	Number of Supervisors	1 (First Shift) + 1 (Second Shift) + 1 (Third Shift)
	Working Hours	8 hours per shift
Network Operations Center	Number of Users	4 (First Shift) + 4 (Second Shift) + 2 (Third Shift)
	Working Hours	8 hours per shift x 3 Shifts
Security Operations Center	Number of Users	4 (First Shift) + 4 (Second Shift) + 2 (Third Shift) L1 at least 3 and L2 at least 2 and L3 on-demand basis.
	Number of Supervisors	1 (First Shift) + 1 (Second Shift) + 1 (Third Shift)
	Working Hours	8 hours per shift x 3 Shifts
Administrators	DBA, Network Admin, Server Admin, Storage Admin, etc.	10 (Primary DC) + 5 (DR)
	Working Hours	8 hours per shift x 3 Shift
Internal PSA application users	25	One Shift

Parameter	Description	Sizing Estimations
Internal PSA non-application user	50	One Shift
DMS Users	10	One Shift
Dashboard users	25	One Shift
Internet Subscriber	No. of Internet Users	47% (Dec 2018) based on SWS survey ~ 50 Million
Estimated Users	No. of Internet Subscribers	10% of Internet Subscribers
Concurrency Citizen	Concurrent Users	0.5% of the estimated users
Fixed Registration Centers	PhilSys Fixed Registration Center	250
PFRC Desktops	250 desktops	One desktop to be installed in each of the PhilSys Fixed Registration Centers to provide PhilSys services to the Citizens.
Workload Volume	Number of Registrations Per Day Per Kit	35 registrations per day per kit

4.6 Technical Parameters

Table 9. Technical Parameters

Parameter	Description	Sizing Estimations
Network Connectivity *(For future usage the router sized for 2-5 Gbps is recommended)	Network Connectivity (DC-DR Replication Link). The link and / or including bandwidth connectivity shall be provided by PSA or its nominated agency	Dual links of 1 Gbps capacity
	Distance between DC and DR based on Google map	180 kms
	Network Connectivity (Primary DC, Secondary DC and DR Site link) The link and / or including bandwidth connectivity shall be provided by PSA or its nominated agency	Dual links of 500 Mbps capacity
	Network Connectivity (Internet) at the Data Center. The network link / bandwidth will be provided PSA	Initially 200 Mbps internet connectivity
	Network Connectivity (Data Validation) at the Data Center	Initially, 200 Mbps leased line
	Network Connectivity (TSPs) at the Data Center	To be provisioned by respective TSP, based on their transaction projections
DC Power	DC Power per rack	13 to 15 kva
CPU	Utilization upper limits	60% only for non-ABIS component
Re-size / headroom	Virtual Cores, Memory, and Storage Seamlessly	25% of the base capacity, only for non-ABIS components in permanent Data Center
Storage	Static & Transaction data	20 % head room on calculated capacity
Recovery Time Objective (RTO) and	For Pilot, the DC-DR will be in the same city. Subsequently, the DC and	Please refer to the SLA (annex). **Error! Reference source not**

Parameter	Description	Sizing Estimations
Recovery Point Objective (RPO)	DR will be more than 100 KMs apart	**found.Error! Reference source not found.**
Data retention	PSN Data	Always
	Biometric data	Always
Backup window	Incremental data back up every day and full back up every week	6-8 hrs.

4.7 PhilSys Web Portal Sizing Requirements

Table 10. PhilSys Web Portal Sizing Requirements

Parameter	Description	Sizing Estimations
Internet Subscriber	No. of Internet Users	47% (Dec 2018) based on SWS survey ~ 50 Million
Estimated Users	No. of Internet Subscribers	15% of Internet Subscribers
Concurrency Citizen	Concurrent Users	0.5 % of the estimated users
	The peak of Concurrency users	1.0 % of estimated users

4.8 Performance and availability requirements

Table 11. Performance and availability requirements

	Item	Description
1	Maximum processing time – Registration request	No daily backlog i.e. maximum of 24 hours at peak load
2	Maximum response time – biometric authentication request	0.5 second (measured in/out the ABAS)
3	Uptime and availability-De-duplication service	99.5% uptime evaluated on monthly basis on 24x7 service window (for more details, please refer to the SLA provided in annex)
4	Uptime and availability-Authentication and OTP services	99.9% uptime evaluated on monthly basis on 24x7 service window (for more details, please refer to the SLA provided in annex)
5	Estimated Authentication volumes	1.8 million per day

5 High-Level Scope of Work

The following sections provide an overview of the scope of work of the SI.

5.1 Software development

The bidder MUST include all costs related to software design, development, customization, integration, configuration, testing, and deployment (as well as permanent licenses for all required COTS software) in its financial proposal.

The bidder MUST include all COTS software items in the **Summary of Costs (refer to FPF 2)** as part of the bidding documents. The same **Summary of Costs (refer to FPF 2)** will be assessed in the frame of the technical evaluation of the bids.

Table 12. Overview of the scope of work (software development)

#	Scope	Sections	Brief Scope Description
1.	Supply, Installation, Commissioning of Software Systems	Sections 6 and 7	The SI is responsible for the supply, installation, commissioning and maintaining the IT software systems required for the PhilSys Information System in the Primary Data Center and Disaster Recovery and Secondary Data Center. The software applications to be developed by the SI MUST comply with all requirements given in Section 5.4 Exclusions The following items are out of scope for the SI: • Mobile Registration Kits including OS and COTS • ABIS software and hardware for deduplication, Manual Adjudication System and biometric SDKs • PhilID cards personalization systems (card printers, QA workstations, etc.), services and consumables (pre-personalized blank cards, inks, overlays, etc.) • PhilID cards delivery/shipping • Provision of network links (e.g. WAN, Internet connections) • Software to be deployed at Relying Parties (except for the pilot application to be deployed at PSA and DSWD)

#	Scope	Sections	Brief Scope Description
			• PhilSys systems' operators and administrators • SLA monitoring (service) • Site preparation for PFRCs (location, contracts, payments, and fit out) • Central sites (Primary DC, secondary DC, DR) and utilities. The PSA shall provide the physical space for hosting IT Infrastructure in a Primary Data Center and Disaster Recovery site as well as Secondary DC. • Telecommunication costs (SMS) • Management of Partner Contracting (registration) - for onboarding of TSPs and RPs • Authentication device management (registration) - conformance procedures • Payment service provider fees (a payment Gateway is to be jointly identified by PSA/PhilSys and DOF) • ISO/IEC 27000 series certifications from an accredited body Functional Requirements and under Section 7 Technical Solution Requirements – PhilSys Information System. The SI MUST integrate all back-end PhilSys applications including the design and implementation of final workflows. Accordingly, SI shall prepare detailed design and solution architectures such as server architecture, network architecture, database architecture, security architecture, deployment architecture. The SI MUST maintain all software items (including COTS) throughout the duration of the contract.
2.	Integration with BioSP Solution	Sections 6 and 7	Provide integration with biometric SDKs provided by the BioSP for PhilSys front-end systems (registration

#	Scope	Sections	Brief Scope Description
			client) and back-end services (e.g. biometric 1:1 matching SDKs for fingerprint, iris and face).
3.	Software Development Lifecycle, Implementation & Customization	Section 9 and Section 13	PSA has envisaged a Phased implementation roadmap as under: Phase I PhilSys System Application Version_ 1 Phase II PhilSys System Application Version_2 Phase III PhilSys System Application Version_3 Phase IV PhilSys System Application Version_4 The implementation of PhilSys Application shall span across the following stages of software development lifecycle: • Requirements Gathering • Design • Development and Customization • System Testing/ Integration Testing/ Performance Testing • UAT • Release • Continuous Build (Continuous Integration / Continuous Deployment) • Enhancement and augmentation • Technical Support, Troubleshooting, Identification and Resolution • Change and Version Control • Patch Release Management • Deploy application • Offshore set-up of Development and Test Environment including required tools, and • L1, L2 and L3 support for PhilSys application including for MOSIP modules.
4.	MOSIP Application Suite	Section 9	• The SI shall use MOSIP applications suite to satisfy the requirements for the PhilSys core modules. • The SI shall be responsible for configuring the MOSIP application suite to comply with PhilSys requirements.

#	Scope	Sections	Brief Scope Description
			• The PSA and its appointed party will assist in resolving the L3 issues for MOSIP modules.
5.	Implementation and Customization of MOSIP	Section 9	• MOSIP comprises of the following applications: o Pre-Registration o Registration Software Application o Identity Management System o Authentication Solution o PSN/PCN Generator o Partner and Device Management o Integration Middleware • The SI may use the necessary MOSIP documentation (detailed features, functions, processes, and product specifications) from the MOSIP team and / or https://github.com/mosip. • The SI shall re-assess the requirement of MOSIP components and suggest customization of the application, if any. • The SI shall be responsible for providing an API gateway and its integration with MOSIP. • The SI shall be required to integrate the MOSIP components with the PhilSys Information System. • A different vendor (BioSP) shall provide biometric solution. The BioSP shall be primarily responsible for the integration of ABIS with PhilSys back-end systems however the SI will support the integration.
6.	Customization of COTS/OTS Application	Section 9.2.1	The SI shall be responsible for application development and customization of the following, but not limited to, COTS/OTS applications: • Business Intelligence and Data Analytics • Customer Relationship Management • Card Management System • Document Management System • Identity and Access Management

#	Scope	Sections	Brief Scope Description
			• Requirement gathering, design, development and customization and testing of the following support applications: • PhilSys Web Portal and Mobile Application • Customizing the reference Partner and Device Management to meet PSA requirement • TSP and RP Application • Fraud Management System • Knowledge Management System
7.	Pilot client application for online authentication	Section 7	• Design, develop and roll out a pilot authentication client software to support two (2) priority use cases initially identified as (1) PSA Civil Registry and (2) DSWD cash transfer beneficiaries.

5.2 Hardware and consumables

The SI MUST supply, commission and install all hardware (such as, but not limited to: servers, network equipment, HSMs, workstations, racks and peripherals such as screens, keyboards, KVM, etc.) required to run all PhilSys back-end applications mentioned in this TOR (core and support) as well as all COTS that will be developed/customized by the SI, for all environments (test, pre-production, production, backup, etc.), at all central sites (primary DC, secondary DC, DR site, Card Production Site and technical helpdesk), in order to run operations at scale and in accordance with the SLA (see Annex G).

The bidder MUST include all hardware items (including quantities, brand/models) in the **Summary of Costs (refer to FPF 2)** as part of the bidding documents. The same **Summary of Costs (refer to FPF 2)** will be assessed in the frame of the technical evaluation of the bids.

Table 13 - Overview of the scope of work (hardware)

#	Scope	Sections	Brief Scope Description
1.	Supply, Installation, Commissioning of IT infrastructure and Software Systems	Section 8	The SI is responsible for supplying, installing and commissioning the IT hardware and peripherals including network equipment required for the PhilSys Information System in the Primary Data Center, the Disaster Recovery and Secondary Data Center. The details of the hardware and infrastructure requirements are provided in Section 8. The hardware and peripherals to be provided must

#	Scope	Sections	Brief Scope Description
			be verifiable (appearing in an international, reputable (bad or good) source i.e. Gartner, Forrester, G2 Crowd, PCMag, etc.). Hardware should be off-the-shelf and based on open technologies and standards.
2.	Setting Up of Fixed Registration Centers	Section 9.3 Section 8	The SI shall perform the following activities: • Provide 250 sets of Wi-Fi ready desktop computer with UPS, authentication devices (Iris, Fingerprint and Facial), Printer and peripherals for the handling of non-registration transactions. Desktop systems must be delivered complete with the necessary office productivity tools and remote desktop capabilities. • Networking devices for PhilSys Fixed Registration Centers. • Provide hardware and software for Queueing System in all 250 PFRCs
3. .	Network equipment for priority use-cases	Section 7	• Multi-Protocol Label Switching (MPLS) router for the pilot at first two RPs/TSPs (PSA and DSWD).
4.	Other consumables	Section 9	• Consumables for data backups • Individual hardware devices (e.g. USB security keys/tokens) for PhilSys users login, if needed or as suggested by the SI's proposed solution (please refer to section 7).

5.3 Other services

Table 14. Overview of scope of work (other services)

#	Scope	Sections	Brief Scope Description
1.	Project Management & Governance	Section 10	• The SI shall be responsible for managing the engagement and ensure that the deliverables meet the satisfaction of the PSA. • The SI shall be responsible for, but not limited to, the following activities: o Set-up of project management office (PMO); hire and/or mobilize individuals, set up and manage teams. o Manpower deployment in accordance with the plan o Define an Escalation Matrix o Preparation and maintenance of a project monitoring software outlining project activities and milestones. o Change Control Management o SLA Monitoring and reporting o Project Status Monitoring and Reporting o Risk and Issue Management o Exit Management
2.	Setting Up of Registration Centers	Section 9.3	The SI shall perform the following activities: • Set-up of network connectivity at Fixed Registration Centers. • Porting of Registration Software into 5,000 registration kits • Deploy and Commission of 5,000 Registration Kits at 250 PFRCs. • Carry out sample registration in the lab for testing with the help of PSA team • Creation of content and training of Master Trainers for Registration Software. • Setup of PFRC's Queueing System
3.	Technical Services	Section 9	• Integrate biometric SDKs provided by the BioSP with PhilSys front-end systems (registration

#	Scope	Sections	Brief Scope Description
			client) and back-end (e.g. biometric 1:1 matching SDKs for fingerprint, iris and face). • Warranty and Annual Technical Support • Manage Multiple Environments • Asset management • Field Network Assessment • IP Address Management • SMS Services management • SOC Setup and Services management • NOC Setup and Administration • Call Center Setup and Administration • Technical Helpdesk • Manage email gateway • Periodic (Monthly) accuracy test of the automated matching for all biometric modalities of both the ABIS (1:N) and the ABAS (1:1).
4.	Other Business Services	Section 9 Section 7	• Develop Registration Manual • Develop PhilSys Authentication Framework Document including the PhilSys authentication API • Develop technical documentations • Develop other PhilSys manuals related to services such as Onboarding of Partners, Data Center Operations, SOC, NOC, PhilSys Web Portal, Mobile Application, Business Intelligence and Analytics, Technical Helpdesk, etc. • Migrate registration pilot data (approximately one million records including demographic and biometric data) • Publish and maintain mobile application(s) on the mobile app store(s). • Set-up and support the onboarding and deployment of two (2) priority use cases initially identified as (1) PSA Civil Registry and (2) DSWD beneficiaries.

#	Scope	Sections	Brief Scope Description
5.	Primary Data Center, Secondary Data Center, Disaster Recovery Site	Section 9	• The PSA shall provide the physical space for hosting IT Infrastructure in a Primary Data Center and Disaster Recovery site as well as Secondary DC. • The SI shall be required to take over the sites for hosting IT infrastructure. • The SI shall assess the site(s), prepare a site plan and rack plan for approval of PSA. • The PSA reserves the right to obtain services from SI relating to Data Center and or DC transition and migration. • The SI shall provide one (1) Data Center Migration Services for each of the Primary Data Center, Secondary Data Center and Disaster Recovery Site. • The SI shall be responsible for set-up of PhilSys Information System in the new DC/DR in consultation with the PSA.
6.	Information Security	Section 9.7	The SI shall be responsible for ensuring information security including: • Development of security processes and procedures • Development, documentation, implementation, and maintenance of minimum baseline security standards • Design, documentation, implementation, and maintenance of PhilSys security design requirements • Supply, Procurement, deployment and commissioning as well as operations of all security tools and technologies • Documenting, implementing, as well as obtaining certifications
7.	Operations & Maintenance	Section 9 Section 7.5	The SI shall perform the following activities: • Design, Supply, Installation, Commission, and Acceptance: o Server Services

#	Scope	Sections	Brief Scope Description
			○ Network Services ○ Storage Services ○ Backup and Replication Services ○ Virtual Environment Services • Operations and administration: ○ Management of Primary Data Center and Disaster Recovery site ○ Server and Virtual Services Operations ○ System Administration ○ Storage Administration ○ Database Administration ○ Backup / Replication / Restore / Archival ○ Network Monitoring ○ Security Management ○ Event Correlation ○ IT helpdesk & Incident Management ○ Configuration Management ○ Management of license agreements and system manuals and documentation **PSA reserves the right to deploy its own team for operations and maintenance alongside the SI team.**
8.	Benchmarking, Commission, Acceptance and Go-Live	Section 9.8.1	• Set up benchmark environment in DR site • Undertake benchmark exercise before Go-live • Validate the Application and Infrastructure performance benchmarks and undertake enhancement/augmentation, if required
9.	Manpower Requirement / Deployment	Section 11	The SI shall deploy experienced and skilled manpower. SI shall manage and adhere to the following: • Guidelines for staffing and provisioning of manpower • Replacement of Personnel • Removal of Personnel • Logistical requirement of personnel • Escalation Matrix

#	Scope	Sections	Brief Scope Description
			• Deploy key manpower as per deployment schedule • Follow schedule for knowledge transfer and ensure presence of key resources during knowledge transfer
10.	Training	Section 12	• Prepare training plan with the approval of PSA • Impart training • Set up LMS for continuous training • Design training courses and deploy on LMS • Commission KMS
11.	Implementation Schedule	Section 13	• Undertake Phased development and implementation of PhilSys Application • Software release to be planned in Phased Versions (see Section 13 for details)
12.	Maintenance	Section 9	• Maintenance of all PhilSys Applications including release management and maintenance of different Versions of the Application • Maintenance team off-site • The SI shall be responsible for the first level and second level (L1 and L2) maintenance and management of the MOSIP application suite. • The SI MUST maintain all hardware items throughout the duration of the contract. The SI MUST ensure replacement of faulty hardware to meet the SLA, by provisioning a minimum stock of spare parts for critical hardware, for example.

5.4 Exclusions

The following items are out of scope for the SI:

- Mobile Registration Kits including OS and COTS
- ABIS software and hardware for deduplication, Manual Adjudication System and biometric SDKs
- PhilID cards personalization systems (card printers, QA workstations, etc.), services and consumables (pre-personalized blank cards, inks, overlays, etc.)

- PhilID cards delivery/shipping
- Provision of network links (e.g. WAN, Internet connections)
- Software to be deployed at Relying Parties (except for the pilot application to be deployed at PSA and DSWD)
- PhilSys systems' operators and administrators
- SLA monitoring (service)
- Site preparation for PFRCs (location, contracts, payments, and fit out)
- Central sites (Primary DC, secondary DC, DR) and utilities. The PSA shall provide the physical space for hosting IT Infrastructure in a Primary Data Center and Disaster Recovery site as well as Secondary DC.
- Telecommunication costs (SMS)
- Management of Partner Contracting (registration) - for onboarding of TSPs and RPs
- Authentication device management (registration) - conformance procedures
- Payment service provider fees (a payment Gateway is to be jointly identified by PSA/PhilSys and DOF)
- ISO/IEC 27000 series certifications from an accredited body