6 Functional Requirements

6.1 High Level Functional Overview

PhilSys has three major functions:

a. Register individuals;

b. Manage personal data and credentials of registered persons; and

c. Support online authentications.

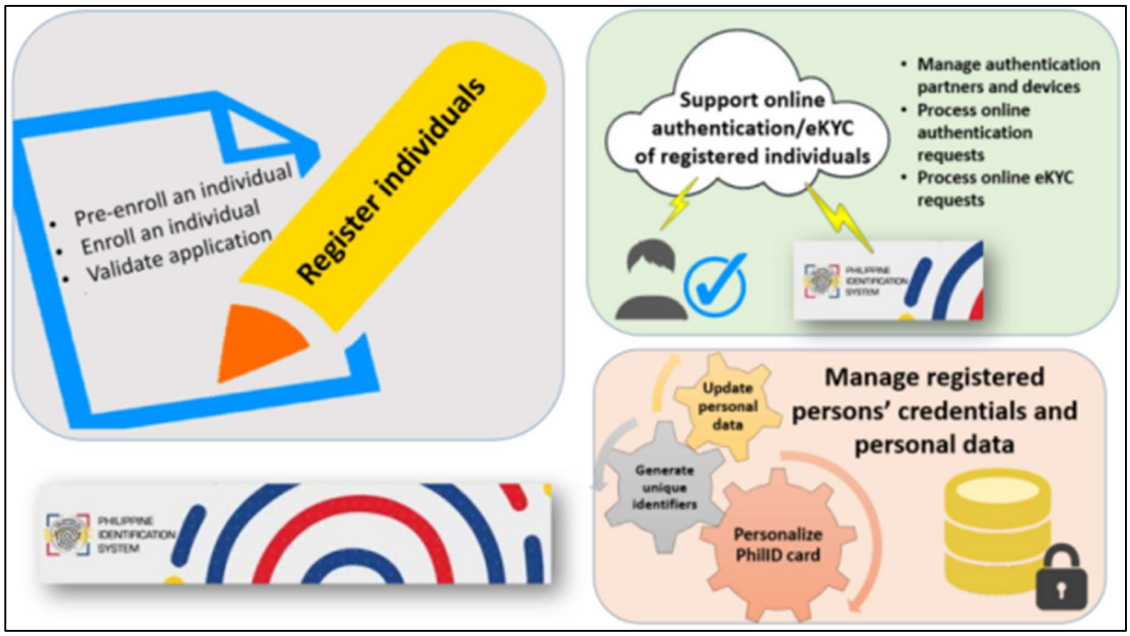

Figure 3. Functional Overview of PhilSys

The PhilSys comprises of multiple separate services integrated together using open standards and APIs. These services are orchestrated to deliver key aspects of the PhilSys such as Registration and Update Processing, the PhilSys Portal, and Authentication Services.

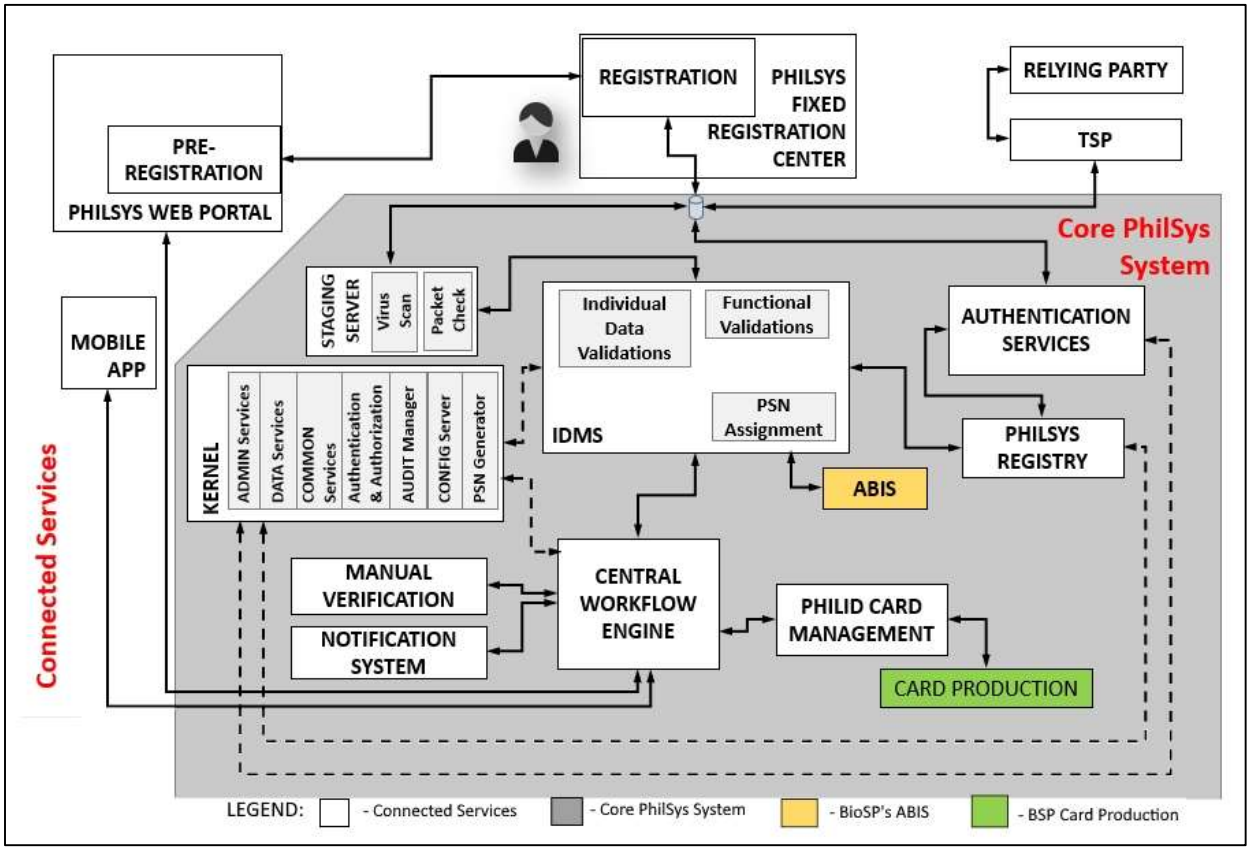

Figure 4. PhilSys High-Level Functional Design

6.1.1 Connected Services

Certain aspects of the functionality required to deliver the PhilSys ecosystem will be delivered by other agencies and will be implemented and managed outside of the core PhilSys Information System. These Connected Services comprise the following:

6.1.1.1 PhilSys Fixed Registration Centers / Mobile Registration Centers

Registration will be phased and comprise of both PhilSys Fixed Registration Centers and Mobile Registration Centers. These centers will capture the demographic and biometric data of individuals who are registering for the PhilSys, presenting this as encrypted registration packets for batch processing by the PhilSys (see Registration Processing). Aside from their registration functions, the PhilSys Fixed Registration Centers will also serve as PhilSys service centers.

6.1.1.2 PhilSys Web Portal

The PhilSys Web Portal is envisioned to be the public-facing facility where PhilSys services are made available online. The PhilSys Web Portal is managed by the PSA where requests are processed centrally in PSA servers. The services available in the PhilSys Web Portal are:

a. Pre-registration and appointment
b. View progress of registration
c. Account creation and authentication
d. View or update demographic data
e. View records history
f. Lock / unlock PSN for authentication
g. Generate and display all active Alyas PSN
h. Request for replacement of PhilID card
i. View card replacement status
j. View FAQs and other PhilSys Information (e.g. locate PhilSys Fixed Registration Centers)
k. Report of lost or stolen PhilID card
l. Submit queries and complaints

6.1.1.3 PhilSys Mobile Application (PMA)

The PhilSys Mobile Application (PMA) is the system used by a Registered Person to access PhilSys services through mobile application. The Mobile Application would require regular network connectivity to PSA Servers for periodic synchronization of data, security patches, and online-only PhilSys services. The Mobile Application is centrally managed by PSA and is published in common mobile application stores, free of charge to the user. The services available in the PhilSys Mobile Application are:

a. Account creation and authentication
b. View or update demographic data
c. View records history
d. Lock / unlock PSN for authentication
e. Request generation and display full “PhilID Card” picture and simple QR code of active Alyas PSNs
f. Request for replacement of PhilID card

g. View card replacement status

h. View FAQs and other PhilSys Information (e.g. locate PhilSys Fixed Registration Centers)

i. Report of lost or stolen PhilID card

j. Submit queries and complaints

6.1.1.4 Relying Parties and Authentication Centers

Relying Parties and Authentication Centers are services dependent on Authentication against the PhilSys Registry enabling them to prove the identity of an individual based on their previous registration with PhilSys. Relying Parties and Authentication Centers will interface directly with the PhilSys Registry or through the Trusted Service Providers (TSP).

6.1.2 Core PhilSys System

The Core PhilSys System provides the core functional elements for the processing of PhilSys applications (registration), generation of credentials (e.g. PSN tokens), authentication against the PhilSys Registry, and management of PhilSys identity data throughout the identity lifecycle.

6.1.2.1 Staging Server

Registration packets created by the registration software will be periodically uploaded on a daily basis to the Staging Server for processing. The packets will be stored in a staging server file system for virus detection before further processing in IDMS and corresponding packet status are created and stored.

6.1.2.2 Identity Management System (IDMS)

6.1.2.2.1 Registration Processing

The Registration Processing module will process batches of registration packets provided by PhilSys Fixed and / or Mobile Registration Centers. Each registration packet will be processed as follows:

a. Decrypt and validate the registration packet

b. Create a temporary PhilSys Record

c. Archive the packet Record in DC and DR

d. Perform a biometric quality check

e. Perform a demographic deduplication

f. Perform a biometric deduplication through ABIS

g. Undergo post-biometric deduplication manual adjudication (if deemed necessary) (ABIS)

h. Undergo manual verification (PhilSys)

i. Request and assign PSN and PhilSys Card Number; and

j. Submit to queue for PhilID Card generation

6.1.2.2.2 Update Processing

a. Registered persons who have their PhilSys credentials will be able to update their demographic and / or biometric information at a PhilSys Fixed Registration Center, or for some demographic data, via the PhilSys Web Portal.

b. For updates sent from the PhilSys Web Portal or PhilSys Mobile Application, the following minimum set of processes is to be performed:

1) Update Demographic Data (configurable by PSA to switch on / off data fields for user updating)

2) If required, submit to queue for issuance / fulfilment (see PhilID Production) – (NOTE: only a change to one or more data items recorded on the PhilID card will trigger a request for a new card to be produced.)

3) Notify the user of status e.g. New Card Requested / Updates Completed

c. For updates sent from a PhilSys Fixed Registration Center, the following minimum set of processes is to be performed:

1) Update biometric data (if present in the packet)

2) Update demographic data (if present)

3) If required, submit to queue for issuance / fulfilment (see PhilID Production) – (NOTE: only a change to one or more data items recorded on the PhilID card will trigger a request for a new card to be produced.)

4) Notify the user of status e.g. New Card Requested / Updates Completed

6.1.2.2.3 Deactivation of PSN

a. The PhilSys law provides deactivation of PSN based on the following grounds:
   1) Upon the request of the registered person. The procedure for deactivation of PSN upon the request of the registered person this is the same as Update Processing.

2) Loss of Filipino citizenship: This is based on the reports coming from DFA or Bureau of Immigration.
3) Loss of resident alien status: This is based on the reports coming from Bureau of Immigration.
4) Death of the registered person: This is based on the reports or death certificates coming from Philippine Statistics Authority (PSA).
5) Failure to submit to initial biometric capture at age five (5) for persons who were registered at age four (4) and below: This is automatically implemented by the system.
6) Failure to submit to biometric capturing at age 15 for persons who were registered at age 14 and below: This is automatically implemented by the system.
7) Presentation of false or fictitious supporting document/s during registration or during application for change of entries: This is based on the investigation reports of PSA-IVID.
8) Misrepresentation in any form during and after registration in the PhilSys: This is based on the investigation reports of PSA-IVID.
9) fraudulent application of the biometric exception: This is based on the investigation reports of PSA-IVID.

b. The PhilID of a person with a deactivated PSN shall be surrendered to the PSA.

c. A deactivated PSN cannot be assigned to another person. Moreover, a person with a deactivated PSN shall not be given a new PSN.

d. The PhilSys notifies the registered person upon the deactivation of his/her PSN.

6.1.2.2.4 Reactivation of PSN

a. The PSA may reactivate the PSN of the registered person upon submission of satisfactory proof for its reactivation under the guidelines to be set by PSA.
b. Reactivation of the PSN shall entitle the registered person to reissuance of PhilID.
c. The PhilSys notifies the registered person upon the reactivation of his/her PSN.

6.1.2.3 PhilSys Registry

The PhilSys Registry is the repository of identity details of all persons registered in the PhilSys. It consists of the PSN, demographic and biometric information of an individual. It is accessed by other PhilSys modules. The PhilSys Master data refers to business-critical data of the PhilSys Information System including the PhilSys Registry.

6.1.2.4 Authentication and eKYC Services

The PhilSys Registry will provide an API for authentication which will support the following methods of authentication:

Table 15. Methods of Authentication

Scope	Sections	Short Description
Biometric Authentication	Unique Identifier: PSN, PCN or *Alyas* PSN Biometric: fingerprint image, iris scan, or facial image (to required standards) eKYC Request: Y/N (default = N)	Incoming biometric data is templated and compared with templates/ images of the same biometric(s) type in the record of the corresponding PSN. Based on the matching threshold, a positive or negative response is returned to the relying party. Response: Success: Y/N Data: eKYC data (if requested and consent legally gained – see notes)
Demographic Authentication	Unique Identifier: PSN, PCN or *Alyas* PSN Demographic: One of the following: Name, Sex, Date of Birth, Filipino/Alien, or Marital Status eKYC Request: No	Incoming demographic data is compared with corresponding demographic data item in the record of the corresponding PSN. Based on the matching threshold, a positive or negative response is returned to the relying party. Response: Success: Y/N

Scope	Sections	Short Description
One Time Password (OTP) Authentication – OTP Request	Unique Identifier: PSN, PCN or *Alyas* PSN eKYC Request: Y/N (default = N)	Where a valid PSN (or equivalent identifier) is received and a mobile number is present in the corresponding PhilSys record, an OTP code will be generated and sent via SMS to the user. Response: OTP-sent: Y/N
One Time Password (OTP) Authentication – Challenge Response	Unique Identifier: PSN, PCN or *Alyas* PSN eKYC Request: Y/N (default = N) OTP code: 6 digit (min) numeric code	The OTP code (6-digit) and PSN are verified to complete authentication. Response: Success: Y/N Data: eKYC data (if requested and consent legally gained – see notes)

Notes:

eKYC Request: Electronically Know Your Customer (eKYC) data will only be available to calling services 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). If enabled by law and the registered person's consent, the relying party will receive through secure transmission specific demographic data and the facial image from the PhilSys following a successful biometric or OTP authentication.

Initially, authentication and eKYC services will be provided to Relying Parties directly by the PhilSys Registry. As volume increases, additional Trusted Service Providers and eKYC service agencies will be introduced to act as nodes or intermediaries.

6.1.2.4.1 Automated Biometric Authentication System (ABAS)

The ABAS will process requests to authenticate individuals against fingerprints, irises or facial images held by the PhilID Registry (see Authentication Services).

6.1.2.5 Automated Biometric Systems Integration (ABIS)

The Automated Biometric Information System (ABIS) performs biometric identification, deduplication, and verification functionalities based on the biometric data captured during Registration. The core features of the ABIS are as follows:

a. Biometric template encoding for fingerprint, face and iris modalities;

b. Biometric identification for fingerprint and iris modalities (1: N search);

c. Biometric authentication for fingerprint, face and iris modalities (1:1 verification) in cases of updates and child registration.

d. ABIS records management.

The ABIS is out of scope for the SI. The PSA has already procured its ABIS. However, the SI must integrate the ABIS to its solution.

6.1.2.6 Manual Verification

The manual verification module is provided to enable authorized PSA staff to review:

a. Incomplete or invalid cases detected before the biometric deduplication.

b. Potentially fraudulent cases raised by the fraud detection system.

c. Potentially duplicated identities identified after biometric deduplication.

6.1.2.7 Notification System

The Notification System manages communication between the PhilSys and the registered persons / clients such as OTP request, SMS, and Email notification.

6.1.2.8 Kernel Services

The Kernel Services provides the core functionalities and services, on top of which the components can be added and built. The Kernel caters to the following services:

a. **PSN and PSN tokens Generation**: This service will receive requests to assign a unique PhilSys Number for the creation of a PhilID, or to create PSN tokens. The Data Services module (see Data Services) will complete the creation or update of PhilSys records.

- Requests for a new unique PhilSys Number will only be passed to the PSNGTMS where a validated and verified unique identification has been completed by the ABIS and controlling Registration Processing module.

- PSA shall provide the PSN format and to the winning bidder. The bidder is expected to use the Number Generator of the MOSIP Application

b. **Configuration Server**: It is a centralized configuration server where all the configuration elements are saved, including the platform configuration and ID Object schema.

c. **Audit and Log Manager**: The Audit Manager component receives a request to audit and store data, validates if the request is from an authorized source, securely stores the requested data and respond back with an acknowledgment of storage (Success / Failure).

d. **Authentication and Authorization**: This service caters to Authentication via web channel (for Pre-Registration web app, Admin web app, and Resident services portal); and Authentication via local system i.e., offline authentication (for Registration Software). It also handles the Authorization of API's accessed via web channel; and Authorization to access specific data.

e. **Common Services**: This allows various PhilSys modules to use common services such as:

   1) OTP Manager
   2) QR Code Generator
   3) Crypto Services (e.g. Cryptography Services, Key Generator, and Management, etc.)
   4) Notification (e.g., OTP Notification Services, Email, and SMS Notification, etc.)
   5) Utilities
   6) Virus Scanner

f. **Data Services**: The Data Services module will maintain PhilSys records containing all PhilSys data elements including the PhilSys Number and provide access to that data to other elements of the solution. The Data Service module will provide the following functionality:

   1) Record Management: for the creation, update and archiving of PhilSys Records.
   2) Data Matching: matching against demographic data to facilitate deduplication.
   3) Data Retrieval: for access to specific PhilSys records.

g. **Admin Services**: This service handles the management of Master Data and PhilSys Fixed Registration Centers including the machines and devices used.

6.1.2.9 PhilID Card Management

The **Card Personalization Management System (CPMS)** is deployed to manage the personalization of PhilID cards (the actual personalization of the PhilID Cards will be carried out by PSA operators using equipment and consumables procured by BSP). The CPMS queues batches of card personalization requests and transmits these to the Card Personalization System for actual printing.

Once the PhilID cards have been personalized, the QA Team under Card Personalization Group will perform quality checks on the cards using the CPMS.

Personalized PhilID cards shall be delivered to designated PhilSys Fixed Registration Centers via PhilSys delivery partners.

The PhilID cards shall be released to corresponding Registered Persons through the PhilSys Fixed Registration Centers. The issuance of the cards shall be recorded in the CPMS.

6.1.2.10 PhilID Production (initial requests and replacements)

The Centralized card production infrastructure will be provided by Bangko Sentral ng Pilipinas (BSP) with card Personalization services operated by PSA, using BSP's physical space,equipment and consumables. The card production capability will include but is not limited to the following functionality:

a. **Card Production**: Preparation of blank cards for personalization. This process includes design and application of different card physical security features, plate production, card lamination, card body punching and card serialization.
b. **Personalization Request Processing**: Verification of electronic requests from the PhilSys Registry for card personalization.
c. **Card Personalization**: Printing of PCN, demographic information, front facing photograph, QR Code (with embedded metadata) and packaging of PhilID in a business size envelope attached to a one-page letter.
d. **Secure Delivery to Subject**: Secure transfer of personalized cards to PhilSys Fixed Registration Centers via Post and Courier Services.
e. **Card Production Reports**: Generation of Card Production Reports (See Annex I for List of Reports).

Based on received requests (and associated data packets) templated PhilID Cards will be personalized and printed for eventual delivery to the registered person. Authorized PSA staff will supervise this personalization process.

6.1.2.11 Post and Courier Services

Secure postal and courier services will be provided for the distribution of PhilID Cards and PhilSys Numbers to PhilSys Fixed Registration Centers as part of the card issuance process. A track and trace facility will be included in this service in order to confirm delivery.

6.2 Logical Layout of PhilSys Design

This section illustrates the logical flow of information across various PhilSys components. The diagrams in this section provide a high-level implementation guide on how each of the underlying PhilSys components and its related processes are sequenced to complete the PhilSys process lifecycles. The diagram also shows that each of the components can be considered as modules (where each of the modules have underlying business logic that are independent from other modules consistent with the modular systems design). Furthermore, these diagrams can be used to identify potential service bottlenecks in each of the processes identified in succeeding sections. This section is segmented into three subsections namely:

1. Registration Processing
2. Authentication Services
3. Other PhilSys Services

6.2.1 Registration Processing

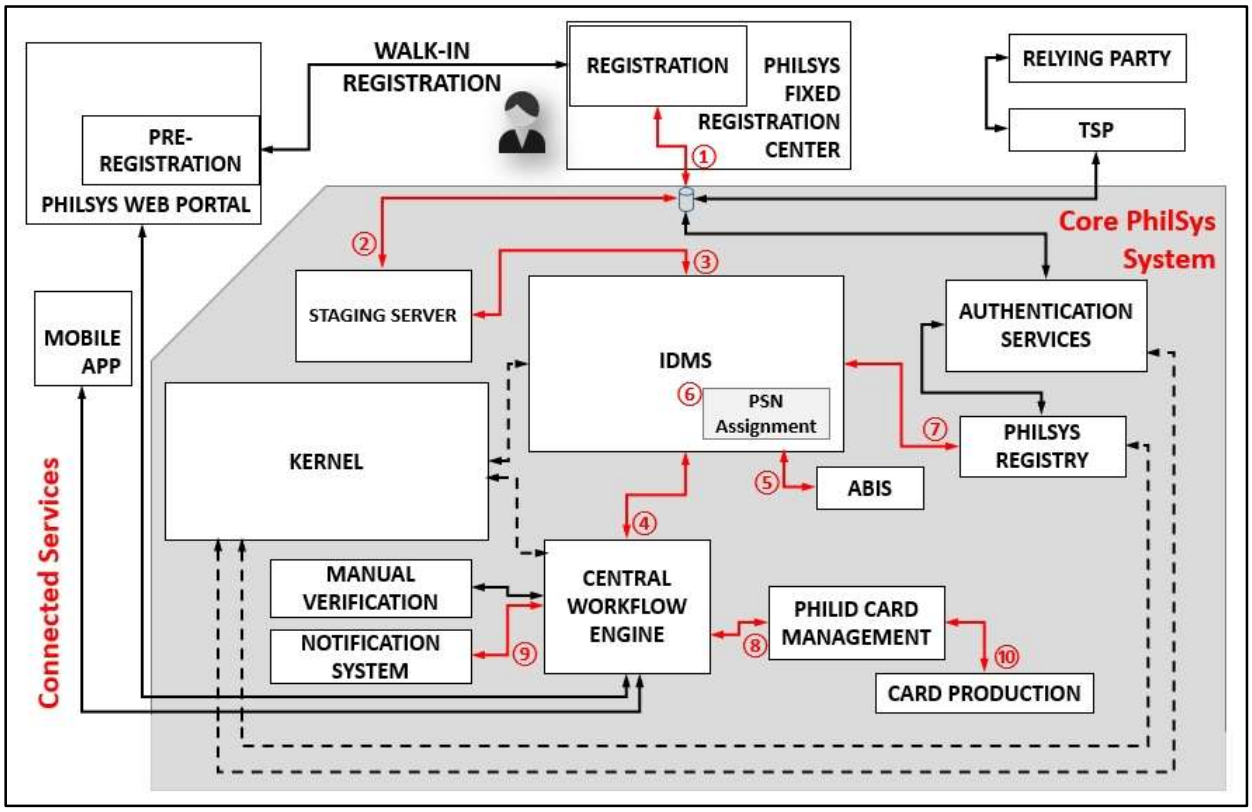

Figure 5. Logical Layout of PhilSys Design – Registration Processing

The logical layout for Registration Processing provides us an overview on how the PhilSys Applicant interacts with the front-end and back-end systems of PhilSys. Applicants in this context refer to Filipinos or Resident Aliens who are applying to be part of PhilSys.

a. Registration starts when the PhilSys applicant submits their demographic and biometric data in any of the PhilSys Fixed Registration Centers or Mobile Registration Centers. Alternatively, the applicant can also submit partial demographic information online via the PhilSys Web Portal and schedule a visit to any of the registration centers and submit their biometric data.

   Upon successful Registration, the applicant receives a Transaction Slip with a Transaction Number that can be used to check the progress of the application, request for assistance or submit complaints to PhilSys via the PhilSys Web Portal or PhilSys Fixed Registration Centers. Data collected from the applicant will be submitted to the back-end systems of the PhilSys Registry for subsequent processing.

b. After successful capture of demographic and biometric data, the registration record is uploaded to the PhilSys Staging Server for validation of registration packet and checking for viruses.

c. Once the data reaches the Identity Management System (IDMS), the registration packet undergoes individual quality validation and functional validations that involve checking of integrity and structure of data packets and quality of individual data and metadata. The IDMS then performs a demographic deduplication process where the submitted demographic data is compared to other demographic data of previously registered persons.

d. Thereafter the packet/ data is forwarded to the Automated Biometric Identification System (ABIS) to identify if the person is indeed unique (known as biometric deduplication or 1:N matching).

e. The ABIS receives the submitted biometric images and performs a deduplication process using the fingerprints and iris images.

   If both the IDMS and the ABIS cannot conclusively identify a unique record or if there is suspected fraud, the applicant's record undergoes a manual verification process. Manual verification involves PhilSys Officers manually reviewing potential duplicates and make a decision on the application request either by: (i) approving the application due to a false positive or (ii) disapproving the application due to the existence of a previous record already in the PhilSys Registry or confirmed fraud case.

f. If the record was found as unique, a permanent PSN will be generated and assigned to the record.

g. Then the registration record together with its assigned PSN is stored in the ID Repository or PhilSys Registry.

h. Generation of PSN for an applicant also triggers the generation of a PCN (PSN token) and the personalization of a PhilID card.

i. Once the PSN is available for the applicant, the status of the registration is updated in the PhilSys Web Portal. Notifications through SMS and email (based on the chosen method by the applicant), must be sent by the PhilSys Notification System.

j. Once the PhilID is ready, the card is transferred to an authorized Post and Courier Service Provider to have the PhilID sent to the PhilSys Fixed Registration Center where the applicant was initially registered. Once the PSN and PhilID is received by the applicant, the registration process lifecycle is deemed completed and closed.

6.2.2 PSN Tokenization Services

The PhilSys must support different types of PSN tokenization, serving different purposes:

6.2.2.1 Front-end PSN tokenization for privacy-preserving authentication/eKYC

Registered users wishing not to disclose their PSN or PCN vis a vis relying parties must be able to generate Alyas PSNs through various channels (such as the PhilSys Mobile Application). Generation of Alyas PSN tokens will be done centrally (PhilSys back-end).
For each new Alyas PSN, the registered user will manually choose a lifetime period (e.g. one-time, one day, one month, etc.) and select a list of core personal data that can be shared by the PhilSys with relying parties using the same Alyas PSN in the frame of an eKYC request.

6.2.2.2 Back-end PSN tokenization for PSN seeding into a relying party's information system

The PhilSys must support the generation and management of back-end PSN tokens i.e. unique PSN tokens specifically created for the sole use of a given onboarded relying party. Which means the PhilSys must automatically translate identifiers used in the frame of authentication/eKYC into these back-end PSN tokens. This is categorized as 'Vertical' PSN seeding.

6.2.2.3 Back-end PSN tokenization for PSN seeding into two or more relying parties' information systems (interoperability)

In an effort to better protect the Registered Users' privacy, the PSA wishes to leverage tokenization (applied to the permanent PSNs) for allowing two or more onboarded relying parties to share personal data or check personal attributes outside of the scope of PhilSys, without having access to the permanent PSNs and via the use of central controls/GUIs. This is categorized as 'Horizontal' PSN seeding.

A high-level solution is introduced hereunder. The Bidder is invited to reflect on the problematic, challenge the suggested model and/or identify other innovative way of achieving the aforementioned objective and share details about the best possible solution in its technical proposal. The proposed solution will be considered in the frame of the technical evaluation of the bids, reviewed during the detailed technical specification phase and ultimately implemented by the SI.

Possible solution:
Each time an online authentication/eKYC request is received (through a TSP), the PhilSys back-end system will check whether it embeds a "context" field. This field indicates whether or not the transaction happens in a given "data sharing" scenario. If so, be it, after a number of checks/validations and if and only if the authentication is successful, it will automatically append a "shared token" to the response that will be sent back to the originating RP.

In order to enable this, the following functions MUST be available to an authorized, dedicated type of PhilSys administrator through dedicated GUIs:

- **Create a new correlation space**
    - A "correlation space" is a logical group of two or more onboarded RPs that have been authorized to use common PSN tokens in order to share personal data or check personal attributes outside of the PhilSys' reach.
- **Add a Relying Party to a correlation space**
    - Find/select onboarded RP, select correlation space and add.
- **Remove RP from a correlation space**
    - Find/select correlation space, display RPs belonging to it, find/select one and remove.
- **Delete an existing correlation space**
    - Find/select correlation space, remove.
- **Rotate shared tokens for a given correlation space**
    - Find/select correlation space
    - Select rotation mode
        - Unit mode: whenever a token belonging to this correlation space is used in the frame of an online authentication or eKYC request, it is automatically substituted with the new one.
        - Batch mode: generate a mapping table linking old tokens to new ones in the form of a file.
        - Launch rotation.

6.2.3 Authentication/eKYC Services

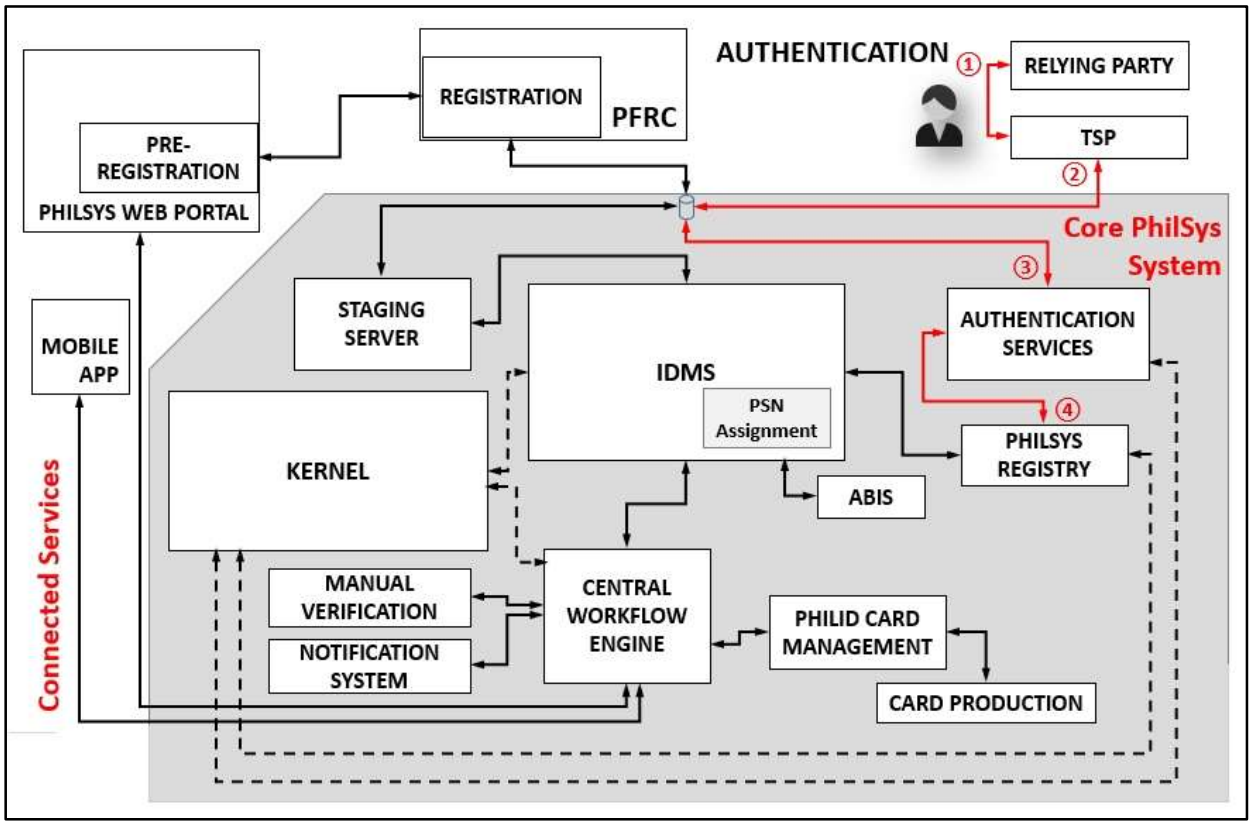

Figure 6. Logical Layout of PhilSys Design – Authentication Services

The logical layout for Authentication Services provides an overview on how the identity of a Registered Person can be authenticated through PhilSys.

a. The Registered Person who comes to a Relying Party (RP) for specified services can be authenticated by the RP after submission of credentials (i.e. a PSN- permanent or token such as the PCN or any Alyas PSN - and one or more authentication factors such as an OTP sent by SMS and/or any of the three biometric modalities, fingerprint, iris, or facial).

b. The RP transmits the authentication /eKYC request through the Trusted Service Provider (TSP) to the PhilSys.

c. Once the authentication/eKYC packet is received at the PhilSys ID Authentication Service, the packet is checked for authenticity of credentials of the Registered Person, RP, and TSP.

d. Then the PhilSys ID Authentication Service fetches the ID and corresponding biometric template from the PhilSys Registry and performs 1:1 matching.

e. The result of authentication is then returned to the RP via the TSP. Once authenticated, the Registered Person receives the services from the RP.

6.2.4 Other PhilSys Services

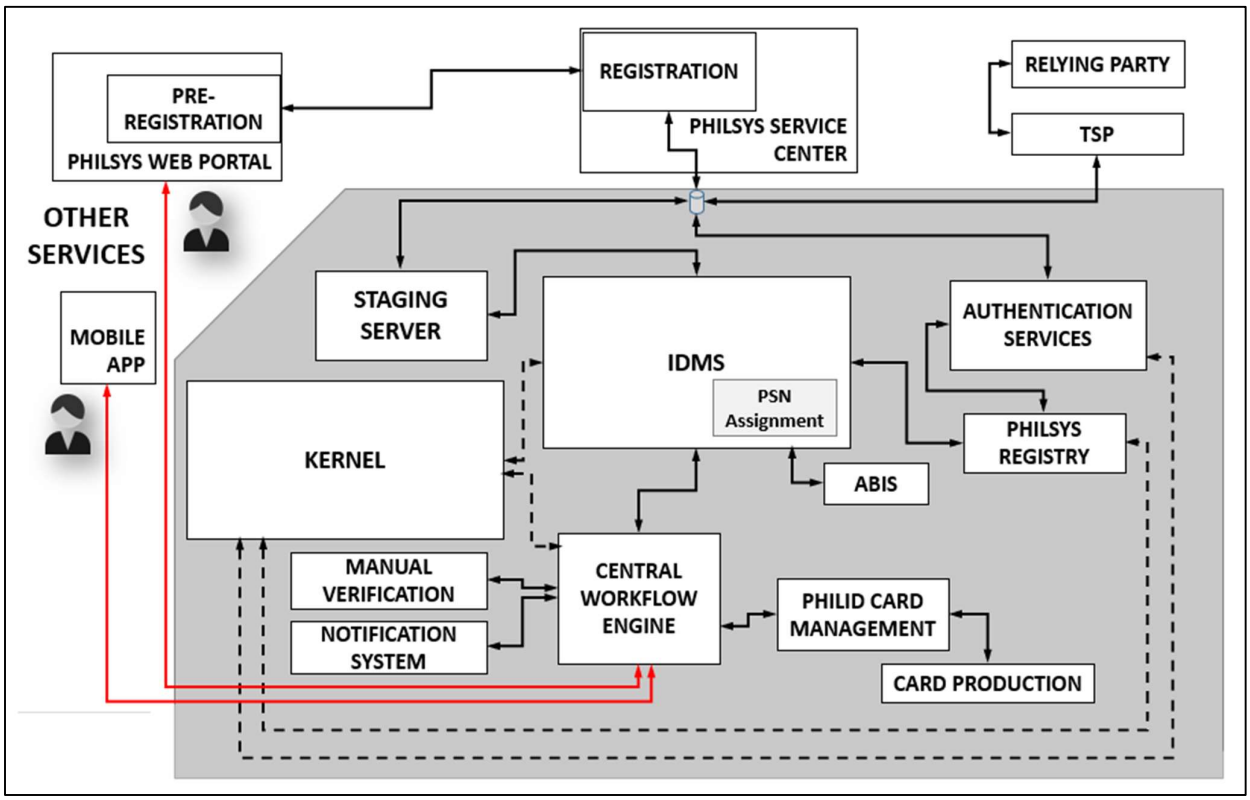

Figure 7. Logical Layout of PhilSys Design – Other Services

The logical layout for Other PhilSys Services provides an overview on how the PhilSys Registered Person access other services provided by PhilSys.

Through the PhilSys Web Portal, Mobile App, and PhilSys Fixed Registration Centers, the registered person can access other PhilSys services such as:

a. Review his or her record history,

b. Set authentication permissions and consent to various authentication requests,

c. Monitor authentication requests on his or her data,

d. Request the issuance of Alyas PSN and

e. Request for PhilID replacement as needed.

6.3 Functional Specifications

This section provides a detailed specification of the manual and automated processes, procedural sequence, activity flows, business logic, and dependencies to complete the six functional requirements of PhilSys.

6.3.1 Pre-registration

6.3.1.1 Pre-Registration process

The following procedure describes the underlying processes and dependencies for registration with an option for the Applicant to submit partial data:

a. The user starts by filling out an electronic registration form. In the case of an applicant, he/she uses the PhilSys Web Portal. If the pre-registration is done by an agent, the latter will either use the PhilSys Web Portal or a pre-enrolment software running on a tablet (possibly in offline mode).

b. After the registration form is temporarily saved into the system, the user uploads scanned copies of the documentary requirements and sets an appointment schedule and chooses a PhilSys Fixed Registration Center where his / her biometrics will be captured. Once all the requirements are submitted, the user receives an appointment reference number that will be presented to the Screener or other staff upon arrival in the PhilSys Fixed Registration Center.

c. On or before the appointment date, the registration kit at the chosen PhilSys Fixed Registration Center receives the partial information of the Applicant from the Pre-Registration Server. This would mean that the PhilSys Fixed Registration Center must have network connectivity with the Central Registration Server. Downloading partial information to the Registration eliminates the need to re-encode information that was previously provided by the Applicant.

d. Upon arrival in the PhilSys Fixed Registration Center, the Applicant presents the appointment reference number to the Marshall. Then the Marshall directs the Applicant to a Registration Officer. The Registration Officer uses the appointment reference number in retrieving the partial information from the Registration Software.

e. The Registration Officer checks if the partially submitted information is complete and consistent with the original copy of the supporting document presented by the applicant. Succeeding processes from this point moving forward is practically the same with the registration process discussed in the previous section (refer to *Section 6.2.1 Registration Processing*). The advantage of the pre-registration process is that it improves the speed and accuracy of encoding the demographic data.

f. The objective of the pre-registration software would be to improve the quality of demographic data capture and reduce the registration time at the registration center. This will also help in increasing throughput of registration centers and reduction of overall registration cost. The pre-registration service will be offered through the PhilSys portal and PhilSys mobile application. This pre-registration application is an optional facility for Filipino residents where they would

have the facility to go for registration with a prior appointment. Residents who do not avail this facility, can still go for registration in any of the registration centers within their vicinity for which Proof of Address is submitted by the resident for registration.

6.3.1.2 Key Functionalities of the Pre-Registration Application

The key functionalities of the Pre-Registration Application are provided below:

a. **Timeslot availability:** The Pre-registration application would maintain a list of available timeslots for appointment at each of the registration centers and would make this available as a real time service via open API's / web services enabling residents to check and make appointments for registration services.

b. **Local device encrypted storage:** The pre-registration system will allow for encrypted local device storage to enable users to store an original version of their submitted data into a local repository. The locally stored encrypted file will only be readable using the same application and credentials used to generate it.

c. **Appointment bookings:** The pre-registration application would provide the facility of making appointment bookings from a set of available slots provided by the timeslot availability feature of the application. The appointment booking would have a feature of booking for one person or more than one family members as a group. In case of group appointment, a separate pre-registration reference number would get generated for each individual.

d. **Location dictionary:** A location dictionary would be available in the pre-registration database and would be geographically associated to the registration centers in the chosen geographical location. Depending on the address of the resident, a list of registration site options suitable to the given address will be provided. The location dictionary would also contain latitude-longitude details for the pre-registration centers for display on the pre-registration web page using public geographical API's from Google, Bing or other GPS/Map services providers.

e. **Demographic data capture:** The application would allow demographic data capture as provided by the resident. Some of the key fields to be entered would be Name, Date of Birth, Gender, Address, Email, Mobile number. The address field would be divided into multiple entry fields where certain information such as Region, Province, Municipality, etc., would be available in the drop box menu.

f. **Document upload:** The application would allow the resident to upload scans of documents to provide Proof of Identity and Proof of Address.

g. **Acknowledgement receipt:** The application would allow the resident to submit details. Once details are successfully submitted, an acknowledgement containing the pre-registration number, chosen registration Center and date/time of appointment would be available for printing. In case the resident has provided a mobile/email, the receipt would be emailed and/or sent via SMS message to the resident.

h. **Available on public internet:** The pre-registration application would be available and accessible as part of the PhilSys Mobile app and PhilSys portal on the web for Philippines residents. The pre-registration facility will also be available to Filipino citizens living abroad. These citizens will be able to submit a request for approval subject to verification from PhilSys.

i. **GPS APIs & Location Services:** The pre-registration web pages would be integrated with geo-IP location-based services that are interoperable with google maps or any other map service provider allowing residents to find the location of the registration Center on the Web. A pre-requisite for this functionality would be that the registration centers be geo-tagged in the pre-registration database.

6.3.1.3 Pre-Registration: User / Actor: Applicant

Table 16. Functional Requirement of Pre-Registration- Applicant

Functional Requirement	Description
Complete Pre-Registration Form	The system MUST provide Applicants with a means of completing an online pre-registration form via the PhilSys Web Portal. This pre-registration form MUST gather demographic details from the Applicant.
Upload Documents	The system MUST provide Applicants with the ability to upload images or PDFs of supporting documents to accompany the pre-registration form.
Choose Appointment Slot and Location	The system MUST provide Applicants with the ability to choose a registration center location, and a date and time slot for the appointment.
Submit Pre-Registration Form	The system MUST provide means to submit a completed form and any attached documents for processing by the PhilSys Information System. Completed forms MUST be checked for completeness and data errors before acceptance for submission. The system MUST provide the Applicant a printable appointment Reference Number.

6.3.1.4 Pre-Registration: User / Actor: pre-enrolment agent

Table 17. Functional Requirement of Pre-Registration- pre-enrolment agent

Functional Requirement	Description
Complete Pre-Registration Form	The system MUST provide pre-enrolment agents with a means of submitting a pre-registration form (including a locally-generated reference number) via a mobile device running a pre-enrolment application that can also work offline. This pre-registration form MUST gather demographic details from the Applicant.
Upload Documents	The system MUST provide the pre-enrolment agents with the ability to upload images or PDFs of supporting documents to accompany the pre-registration form.
Choose Appointment Slot and Location	The system MUST provide pre-enrolment agents with the ability to choose a registration center location and a date and time slot for the appointment.
Submit Pre-Registration Form	The system MUST provide means to submit a completed form and any attached documents for processing through the PhilSys Information System. Completed forms MUST be checked for completeness and data errors before acceptance for submission. The system MUST provide the Applicant a printable Appointment Reference Number (ARN).

6.3.2 Registration Process

This section provides the process for PhilSys Registration and describes the functionalities of the registration software used to enroll individuals into the PhilSys Registry.

6.3.2.1 Registration Software

The function of the registration software would be used to undertake registration at the Mobile / Fixed Registration Center, an open source technology-based software shall be used. This software will be integrated with biometric capturing devices of various manufacturers, which are compliant to identified biometric standards.

The key functionalities of the application are provided below:

a. **Software, User and Configuration Management**: Registration software shall have the capability to configure users and devices to enable administrator and registration officer to login to the system using a Desktop or a Laptop. The registration officer shall login using PSN number only to a mapped device. Necessary configurations would be setup on the desktop/laptop by a registration software admin. These configurations would only be available to the registration software admin and not to a registration officer.

b. **Location and Other Master Data Download**: Location codes and other master data shall be available in the local database of the registration software and shall be regularly synchronized to ensure any changes in the master data are available on the registration software end at all times. This synchronization shall happen automatically either as a push/pull operation through the PhilSys Information System or Registration Software.

c. **Pre-Registration Data and Certificates Downloads**: The registration software shall have the capability to download all the pre-registration data in advance from the pre-registration sever to minimize network transactions during the registration session for residents who availed the pre-registration facility. Registration software shall only allow download pre-registration information of residents who have appointments in that registration center only for that day. For privacy reasons, the documents of the resident will be available for viewing only within the registration software.

d. **Demographic Data Capture**: The application shall allow demographic data capture by the Registration Officer. Data shall be populated from the pre-registration application or through manual data entry by the registration officer based on registration form submitted by the resident.

e. **Document Upload**: The document scan and upload shall happen only through the registration software. The registration kits (digital camera, iris scanner, document scanner, etc.) shall only operate with the registration software.

f. **Biometric Data Capture**: The application shall have the capability to capture biometrics such as fingerprints, iris and photograph of the resident. The biometrics captured shall be checked for quality using biometric quality check APIs and once a minimal acceptable quality of biometric capture is achieved, the registration software shall enable the registration officer to proceed with completion of registration. On completion of registration, a Data Packet will be created to be transmitted to the PhilSys Information System.

g. **PKI Encryption**: All data packets that will be created shall be encrypted using PKI encryption technology and strictly using PH root certifying authority (CA) certificates – self signed keys will not be allowed. Only public keys are stored in the registration kit and the location is configured by the administrator. The public keys are not accessible to the user for any kind of modification purpose. Audit log information about these keys (Timestamp for creation/update, Hash of the key, etc.) are stored on the PhilSys Information System, so as to enable audit of the registration software PKI keys to detect any tampering of keys. During the registration session, data entered shall be maintained in memory in an encrypted form for enhanced security. All data stored shall be digitally signed by the registration officer using his/her private key.

h. **Local Storage & Secure File Transfer**: Registration software shall have the capability to store information such as master data and registration packets in a secure fashion. The Registration software shall have a database where all information is stored locally. It will also have the facility to securely transfer the registration packets to PhilSys Information System.

i. **Audit Logging**: The audit information such as “who was registered, registration officer information, supervisor information, time taken for registration, location of registration, any exception conditions etc.” will be associated with every registration session which shall be

logged by the registration software. This information would be used to ensure that continuous quality is achieved while registration is carried out. Even mouse clicks and other detailed information could be captured for security auditing and scanning etc. The registration software shall also be capable of a running a scan (triggered from the PhilSys Information System) of the machine on a periodic basis to ensure no fraudulent activity has happened (e.g. tampering the configuration of registration software etc.).

j. **Registration number generation and Receipt print**: Once registration information is collected and packet has been sealed with encryption, an acknowledgement number is generated, and a receipt can be printed and handed to the resident.

k. **Secure Sync**: A secure synchronization with PhilSys Information System shall enable the registration packets to be transferred to the PhilSys Information System in a secured fashion.

l. **Quality Management**: To ensure biometric de-duplication and authentication, the captured biometrics should be of good quality. For ensuring that good quality biometrics are captured by the Registration Software, there shall be quality assurance components in the Registration Software. These components will use biometric quality check APIs.

m. **Capability to address Exception Conditions**: The registration software shall have the capability to address exceptional conditions such as handling persons who are handicapped, people with poor quality of biometrics, people without any documents, etc. While the normal default behavior would be to capture all the biometrics, in case a person is handicapped, the Registration Software should permit the Registration Officer to override the default behavior using a manual override. In such case, a photograph of the person showing handicapped hands shall be captured.

6.3.2.2 Registration Procedure

a. The process starts from the Applicant where documentary requirements and an accomplished registration form are submitted to the Screener in the PhilSys Fixed Registration Center.

b. A Screener receives the submitted documents and checks for completeness and consistency of the data present in the documents. If the documents are found in order, the Screener forwards the application to the Registration Officer. If the documents are inconsistent or incomplete, the Screener notifies the Applicant that the documents are rejected and provides the reason for the rejection. For Introducer-based Registration, the registration officer captures the PSN of the Introducer. Qualified Introducer can vouch for at most 15 applicants per year.

c. Once the registration officer receives the documents from the Screener, the Registration Officer selects the New Registration option and encodes the data from the registration form into the PhilSys Registration Software. As the Registration Officer encodes the information, the applicant can see, in real time, what is being entered into the system, using the second monitor that is part of the registration kits. Through this approach, the applicant can check for consistency and notify the Registration Officer of any data corrections.

d. After the data is encoded onto the registration software, the Registration Officer requests for the Applicant's biometrics through biometric capture devices. Biometrics capture includes 10 fingerprint images, 2 iris images and 1 facial image.

e. An automated biometric capture data quality check informs the Registration Officer if the biometric images already complies with the minimum quality standards set by PhilSys. If any of the biometric images fail this quality check, a number of recapture attempts is required. If the Applicant cannot provide the biometric image or any attempts at recapture fails, the Registration Officer notes into the registration as biometric exceptions (For Handling of Biometric Exception Process, see Annex B).

f. After the biometric information requirements are captured into the Registration Software, the Applicant reviews and approves the demographic and biometric data for subsequent PhilSys processing. If the Applicant does not approve of the encoded demographic and biometric information, the registration officer reverts to the Applicant's information needing revisions.

g. After the Applicant's approval, the Registration Officer biometrically signs the Applicant's data into a data packet, complete with metadata that will be included in the Applicant's record history. A transaction number is issued to the Applicant as proof that the application is confirmed. This transaction number can be used by the Applicant to track and check the status of the application, submit complaints or request for more information regarding his / her application.

If secured connectivity is available, the data packet is transmitted to the PhilSys Registry. If the PhilSys Fixed Registration Center or Mobile Registration Center does not have Internet connectivity the packets are prepared, secured and uploaded by batch once connectivity is made available. Once the data packets are successfully uploaded, the PhilSys Registry replies with a confirmation message back to the Registration Software. This confirmation message plus the notification that the registration packets have been successfully reduplicated and assigned respective PSNs shall trigger the deletion of the local copies of the data. The data packets shall be stored in the kits for a minimum of 60 days.

6.3.2.3 Registration: User / Actor: Applicant

Role: To complete a PhilSys registration and apply for a PhilID.

Table 18. PhilSys Registration Functional Requirements

Functional Requirement	Description
Submit Demographics	The system MUST be able to capture the Applicant's demographics and to store them in a standards-based format for transmission to the PhilSys Registry for subsequent processing.
Submit Biometrics	The system MUST be able to capture the Applicant's biometrics and to store them in a standards-based format for transmission to the PhilSys Registry for subsequent processing.
Review and Sign-off	Applicants MUST be provided with the ability to review demographic and biometric data gathered during the registration process and confirm (i.e. sign-off) the registration as ready for processing.
Get Transaction Number	The system MUST be able to issue a Transaction Number following a successful (completed) registration. This Transaction Number will be used to track the progress of each application by the applicant via PhilSys Web portal or by the PSA using the back-end processes.

6.3.2.4 Registration: User / Actor: Registration Officer

Table 19. PhilSys Registration Officer Functional Requirement

Functional Requirement	Description
Retrieve Pre-Registration Information	In the case of a pre-registration, the Registration Officer MUST be provided with the ability to retrieve a pre-registration form / documents submitted by the Applicant via the PhilSys Web Portal. The pre-registration form and uploaded documentation will be retrieved by the Registration Officer entering the Appointment Reference Number or name of the Applicant.
Encode Information from Registration Form (Walk-in)	For paper-based applications, the system MUST provide a data entry mechanism for the contents of the application form and scan supporting documents.

Functional Requirement	Description
Perform Data Quality Checks	For biometric data captured during registration the system MUST provide the ability to review the quality of data captured and to confirm this with the Applicant as necessary.
Prepare Data Packet for Submission	Once all data has been captured and data quality checks completed, the system MUST provide the Registration Officer with the ability to finalize the application and use his/her private key to sign-off and create a data packet for submission to the PhilSys Registry for processing.
Print Transaction Number	A Transaction Number MUST be issued following a successfully completed registration. This Transaction Number will be used to track the progress of each application by the applicant via PhilSys Web portal or by the PSA using the back-end processes.

6.3.3 Updating Process

The updating process facilitates the updating of demographic and biometric data of registered persons. The procedure is similar to the registration process.

a. The process starts from the registered person where documentary requirements and an accomplished registration form indicating update of personal data are submitted to the Screener in the PhilSys Fixed Registration Center.

b. A Screener receives the submitted documents and checks for completeness and consistency of the data present in the documents. If the documents are found in order, the Screener forwards the application to the Registration Officer. If the documents are inconsistent or incomplete, the Screener notifies the Applicant that the documents are rejected and provides the reason for the rejection.

c. Once the registration officer receives the documents from the Screener, the Registration Officer selects the update transaction option and encodes the data from the registration form into the PhilSys Registration Software. As the Registration Officer encodes the information, the registered person can see, in real time, what is being entered into the system, using the second monitor that is part of the registration kits. Through this approach, the registered person can check for consistency and notify the Registration Officer of any data corrections.

d. After the data is encoded into that registration software, the Registration Officer requests for the registered person's biometrics through biometric capture devices. Biometrics for capture[2] includes fingerprint images, iris images and facial image.

[2] Refer to Section 5c of the Philippine Identification System Act (RA 11055)

e. An automated biometric capture data quality check informs the Registration Officer if the biometric images already complies with the minimum quality standards set by PhilSys. If any of the biometric images fails this quality check, a number of recapture attempts is required. If the registered person cannot provide the biometric image or any attempts at recapture fails, the Registration Officer notes into the registration as biometric exceptions. For Handling of Biometric Exception Process, see Annex B.

f. After the biometric information requirements are captured into the Registration Software, the registered person reviews and approves the demographic and biometric data for subsequent PhilSys processing. If the registered person does not approve of the encoded demographic and biometric information, the registration officer reverts to the registered person's information needing revisions.

g. After the registered person's approval, the Registration Officer uses his/her private key to sign-off registered person's data into a data packet, complete with metadata that will be included in the registered person's record history. A transaction number is issued to the registered person as proof that the request for update is confirmed. The registered person to track and check the status of the request for update, submit complaints or request for more information regarding his / her application can use this transaction number.

If secured connectivity is available, the data packet is transmitted to the PhilSys Registry. If the PhilSys Fixed Registration Center does not have Internet connectivity the packets are prepared, secured and uploaded by batch once connectivity is made available. Once the data packets are successfully uploaded, the PhilSys Registry replies with a confirmation message back to the Registration Software. This confirmation message plus the notification that the update packets have been successfully implemented shall trigger the deletion of the local copies of the data.

Since the Updating Process uses the same system and procedure that are employed in the Registration Process, the functional requirements for PhilSys Registration Officer for Updating Process is identical with that of Registration Process.

6.3.4 Deduplication Process

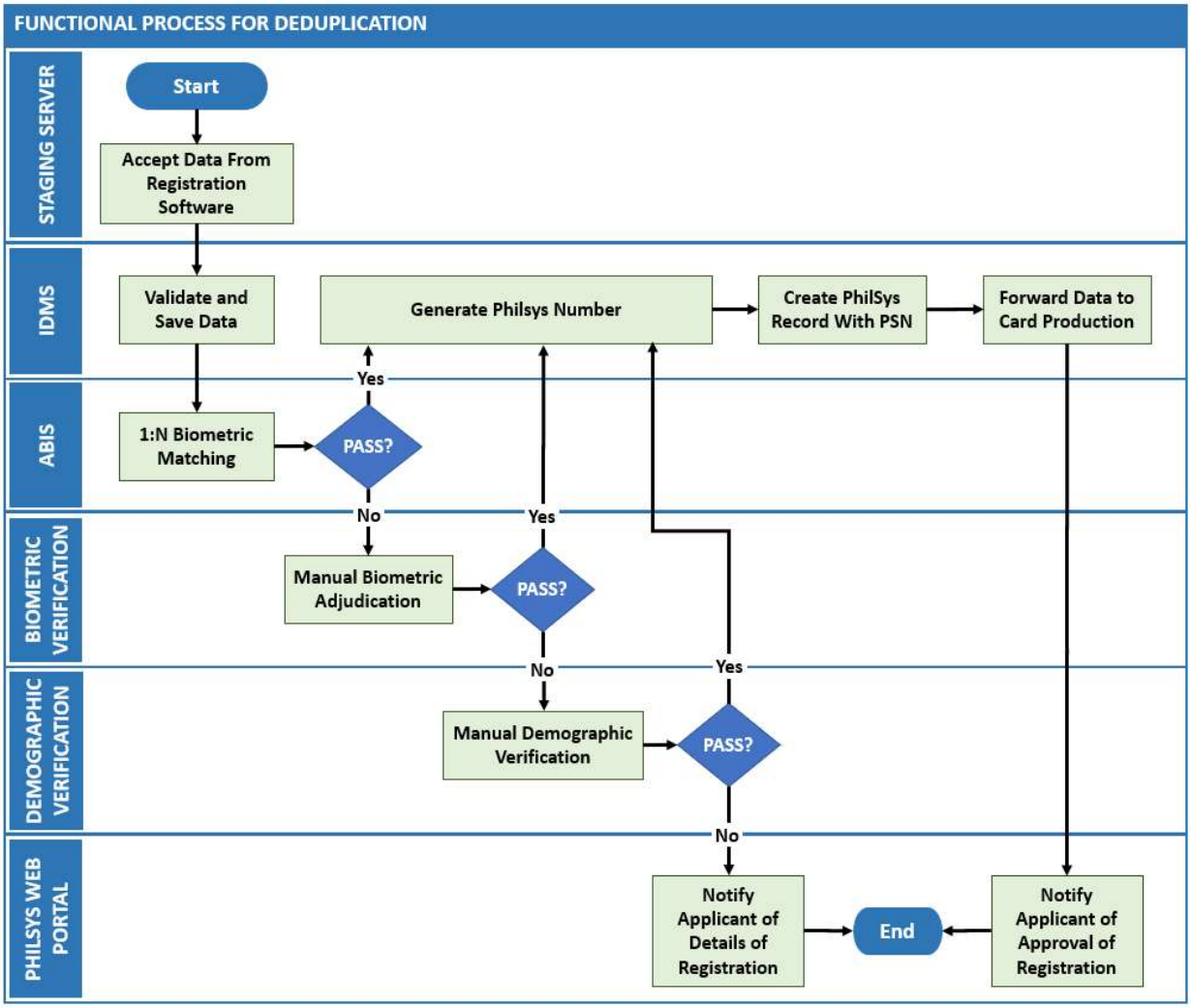

Figure 8. Deduplication Process

The process diagram above shows the underlying processes and dependencies for deduplication process. The primary goal for deduplication is to ensure that the Applicant is indeed unique, and that the Applicant does not already have a record in the PhilSys Registry. All the processes illustrated above are mainly facilitated by PhilSys / MOSIP applications and are mostly automated in nature.

a. The process starts from the Staging Server where the registration data packets are uploaded into from various registration kits are aggregated. The Staging Server verifies the packets and forwards these to the IDMS.

b. The IDMS saves the demographic data and related metadata into a distinct data store and validates the contents in the data packets. Furthermore, the IDMS sends the biometric images to the Automated Biometric Identification System (ABIS) for 1: N matching.

c. If a registration record is found unique by ABIS, a PhilSys Registry record is created and corresponding PSN will be generated.

d. In the event of other records potentially matching the application are found, a two-type Manual Verification process follows:

   1) **Biometric Manual Adjudication** involves PhilSys Investigators reviewing the biometric images of potential matches.

   2) If there are still potential matches during Biometric Manual Adjudication, **Demographic Manual Verification** is performed. This involves PhilSys Investigators checking on demographic data match scores of potential matches. Results from the biometric manual adjudication and demographic manual verification shall be used by the IDMS to assert uniqueness of the Applicant in the PhilSys Registry.

e. If the record that underwent manual verification is unique, the registration record is inserted into the ABIS gallery. A corresponding PhilSys Registry record, PSN and PhilSys Card Number (PCN) will be generated.

f. Otherwise, the Applicant will be denied and tagged as duplicate.

g. Data of unique records with the newly issued PSN will be forwarded to the PhilID card production facility. Moreover, the applicant is notified of the successful registration via the PhilSys Web Portal and other means identified by PhilSys.

6.3.4.1 Deduplication: User / Actor: IDMS

Role: Processing of data packets from IDMS

Table 20. Processing of Registration Packets from IDMS

Functional Requirement	Description
Accept data from IDMS	The IDMS MUST be able to receive secure data packets from the staging server for processing as part of deduplication.
Tag Transaction Number with previously issued PSN	Where a user is found to be trying to register and is already identified within the PhilSys (e.g. due to biometric match), the IDMS MUST associate the Transaction Number with the matched PSN.
Tag Transaction Number with a new PSN	Where the user is found to be unique (with respect to the biometric and demographic data held in the PhilSys Registry), a new PSN MUST be associated with the Transaction Number and the PhilSys Card number (PCN) is generated.
Forward data to Card Personalization and Management System (CPMS)	Where a new PSN has been issued the CWE forwards the registration record to the CPMS for card personalization purposes.

6.3.4.2 Deduplication: User / Actor: Identity Management System (IDMS)

Role: To manage PhilSys identity records, registration applications, and processing throughout the identity lifecycle.

Table 21. Functional Requirement IDMS

Functional Requirement	Description
Save data packets to data vault	The IDMS MUST include functionality to save data packets received from the Staging Server into the PhilSys Registry (secure data vault).
Save demographic data and metadata	The IDMS MUST include functionality to save demographic data and associated metadata to the data vault for a registration.
Save biometric data	The IDMS MUST include functionality to save biometric data for a registration to a dedicated biometric data store.
1: N Demographic Matching	The IDMS MUST provide functionality to enable the matching of demographic data included in a registration packet to all other demographic data held in the PhilSys Registry in order to identify potential duplication. Exact matches and potential matches should be provided as an output of matching.
Generate PhilSys Number (PSN)	The IDMS MUST include the functionality to generate a new PSN for a unique registration.
Send biometric data to ABIS for deduplication	The IDMS must include functionality to forward biometric data to ABIS through API and ABIS middleware for deduplication.

6.3.4.3 Deduplication: User / Actor: Automated Biometric Identification System (ABIS)

Role: Biometric matching against all previously registered PhilSys biometric records.

Table 22. Functional Requirement of ABIS

Functional Requirement	Description
1: N Biometric Matching	The ABIS MUST provide functionality to enable the matching of biometric data included in a registration packet to all other (relevant) biometric data held in the ABIS Gallery in order to detect duplicate matches. A duplicate match will indicate a previous registration of the same individual or a potential mismatch due to accuracy or data error. Note: This is for information purposes only. This is out of scope for SI.

6.3.4.4 Deduplication: User / Actor: Biometric Adjudication

Role: To verify the matching of biometric data against the PhilSys registry where automated matching is inconclusive.

Table 23. Functional Requirement of Biometric Verification

Functional Requirement	Description
Integration to ABIS Automated deduplication and Manual Biometric Adjudication	The ABIS BioSP MUST provide integration on the ABIS Automated deduplication with the IDMS solution. Such solution of SI will be able to process / make use of results coming from ABIS Automated deduplication and manual biometric adjudication.
Manual Biometric Adjudication	The BioSP will provide an interface for an operator to manually compare biometric data provided as part of registration packet to candidate matches identified by the ABIS during 1: N matching.

6.3.4.5 Deduplication: User / Actor: Demographic Verification

Role: To verify the matching of demographic and biometric data against the PhilSys registry where automated matching is inconclusive.

Table 24. Functional Requirement of Demographic Verification

Functional Requirement	Description
Manual Demographic Verification	The SI MUST provide an interface for an operator to manually compare results of demographic deduplication performed by IDMS and biometric matching scores from the ABIS provided as part of a registration packet to candidate matches identified by the automated demographic 1: N matching process. The operator MUST be able to record a positive or negative decision regarding the match status. The SI MUST provide supervisor mode showing complete demographic and biometric details of matching records for determination of uniqueness. For non-supervisor mode, only demographic deduplication scores and biometric matching scores and photos are viewable to the operator. All actor-based decisions should be logged and available for audit action.