6.3.5 PhilID Card Personalization Process

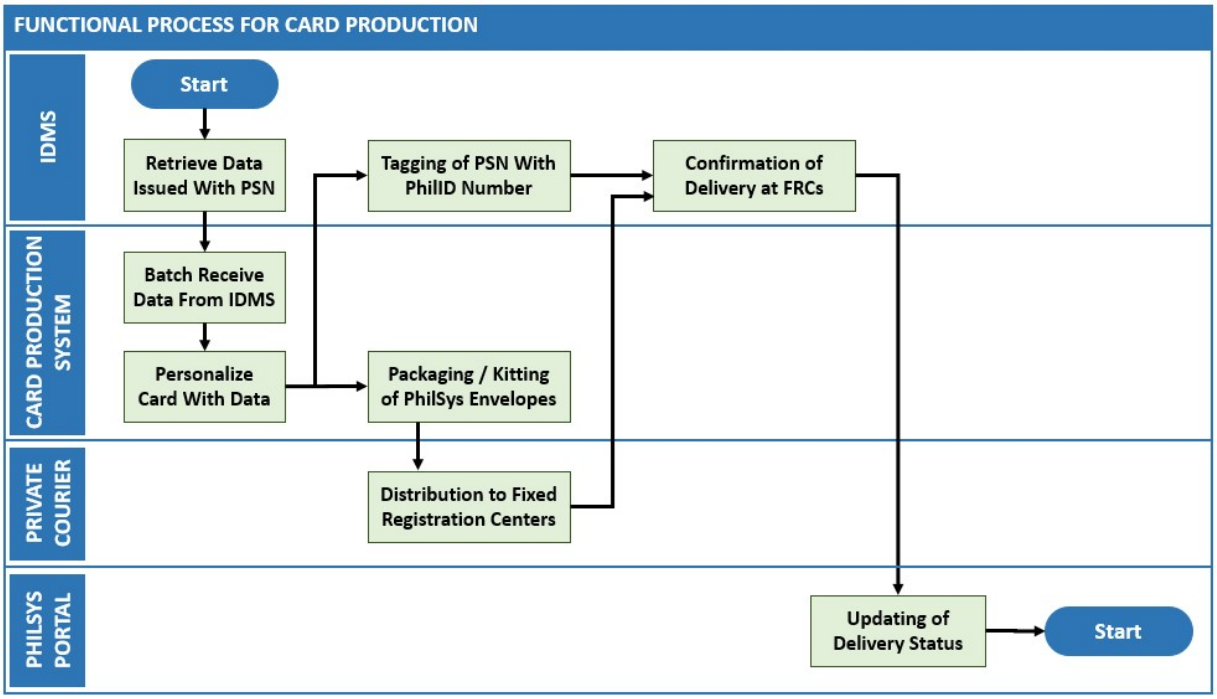
FUNCTIONAL PROCESS FOR CARD PRODUCTION
IDMS
CARD PRODUCTION SYSTEM
PRIVATE COURIER
PHILSYS PORTAL
Start
Retrieve Data Issued With PSN
Tagging of PSN With PhilID Number
Confirmation of Delivery at FRCs
Batch Receive Data From IDMS
Personalize Card With Data
Packaging / Kitting of PhilSys Envelopes
Distribution to Fixed Registration Centers
Updating of Delivery Status
Start

Figure 9. Card Production Process

The process diagram above shows the underlying processes and dependencies to produce the PhilID card and the letter containing PSN. The PSA will manage the personalization and production of the PhilID cards and the delivery of PhilID cards to PFRCs through a third-party courier. While most of the processes happens outside of the PhilSys Registry, it is important to understand how the IDMS interfaces with external systems:

a. The process starts from the PhilSys Registry where the records for card printing are securely stored.

b. The CPMS sends a request for batches of records for card printing to CWE.

c. The CWE forwards the request to Card Batching Utility (CBU).

d. The CBU retrieves the records from the PhilSys Registry, prepares print files, and batches the records for card printing.

e. The CBU forwards the batches of records to the CPMS through the CWE.

f. The CPMS receives the batches of records and queues these into the personalization process.

g. After the cards are personalized and have undergone QA, the CPMS sends information back to the CWE with status, ￼￼the PCN￼￼nput to the Card Management System.x

h. Furthermore, the Card Production Group performs packaging or kitting of the PhilID cards and other communication materials into individual envelopes.

i. These envelopes are forwarded to PFRCs through third party couriers. The PFRCs updates the delivery status of the batches of cards through the CMS.

j. The PFRCs will release to the cards to the clients and update the PhilID card status stored by the CPMS through the front-end (registration) client software.

k. Logs MUST be kept of all Card processing.

6.3.5.1 PhilID Card: User / Actor: IDMS

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

Table 25. IDMS with PhilID Card Personalization Functional Requirements

Functional Requirement	Description
Tagging of PSN with valid PhilSys Card Number (PCN)	The IDMS MUST be able to append a new PhilSys Card Number (PCN) to the PhilSys Registry record associated with the source PSN for personalization and card production.

6.3.5.2 PhilID Card: User / Actor: CBU

Role: To create print files and batch records for card printing.

Table 26. CBU with PhilID Card Personalization Functional Requirements

Functional Requirement	Description
Retrieve data issued with PSN	The CBU MUST be able to retrieve data for card printing from PhilSys Registry.
Create print files and send these to CPMS	The CBU MUST be able to create print files and batch records for card printing and send these to CPMS through the CWE. The print files shall include data (PCN, facial image, labels for two highest quality fingerprints) for QR Code.
Confirmation of Delivery	The Card Production Management System (CPMS) MUST have a mechanism to record the status of delivery of the card and Tag it to the citizen record.

6.3.5.3 PhilID Card: User / Actor: Card Personalization Management System (CPMS)

Role: Personalization and production of PhilID cards.

Table 27. Card Personalization Management System Functional Requirement

Functional Requirement	Description
Receive batches of data from CBU	The Card Personalization Management System MUST be able to receive batches of secure data packets from the CBU through the CWE, store them securely, and manage their use to personalize cards.
Personalize Cards	The CPMS MUST be able to personalize PhilID Cards based on a verified data packet received from the CBU.
Update Status on Quality Assurance (QA) performed on cards	The CPMS MUST enable the Card Production Team to update the status of QA performed on cards. The CPMS MUST provide information to the PhilSys Registry that a PhilID card has been successfully printed for a given PSN.
Packaging / kitting of PhilSys Envelopes	The CPMS MUST have functionality to package, address, and route PhilID Cards (once personalized) to the designated PhilSys Fixed Registration Center.
Notify PhilSys Registry whether or not a PhilID card has been successfully printed for a given PSN.	The CPMS MUST provide information to the PhilSys Registry whether or not a PhilID card has been successfully printed for a given PSN.

6.3.5.4 PhilID Card: User / Actor: Card Production Team

Role: Perform Quality Assurance and delivery of PhilID cards to PhilSys Fixed Registration Centers.

Table 28. QA and delivery status of PhilID cards

Functional Requirement	Description
Distribution to PhilSys Fixed Registration Centers	The Card Production Team MUST be able to update the delivery status of batches of PhilID cards and deliver personalized PhilID Cards to the PhilSys Fixed Registration Centers.
Perform QA on recently printed PhilID cards	The Card Production Team MUST be able to update the status of QA performed on PhilID cards through the CPMS.

6.3.5.5 PhilID Card: User / Actor: PhilSys Fixed Registration Center

Role: Release PhilID Cards to Registered Persons.

Table 29. Releasing of PhilID Cards to Registered Persons.

Functional Requirement	Description
Releasing of PhilID Cards to Registered Persons	The SI must include the functionality of tagging release of PhilID card in the CMS after successful authentication of the card recipient.
Confirmation of Delivery	The PFRC staff is allowed to record the delivery status of batches of cards through the Card Management System (CMS). The SI shall develop the CMS with the functionality that enables recording of delivery status of batches of cards.

6.3.5.6 PhilID Card: User / Actor: PhilSys Web Portal

Role: Public-facing web portal providing access to registration progress and usage information for applicants and registered users accordingly.

Table 30. PhilSys Web Portal Delivery Status

Functional Requirement	Description
Updating of delivery status	The SI MUST create functionality to show the delivery status of a PhilID Card to a Registered Person based on authentication to the PhilSys Web portal.
Card Replacement	The SI MUST create a facility to cater all request for card replacement accessible via PhilSys Web Portal.

6.3.6 Authentication Process

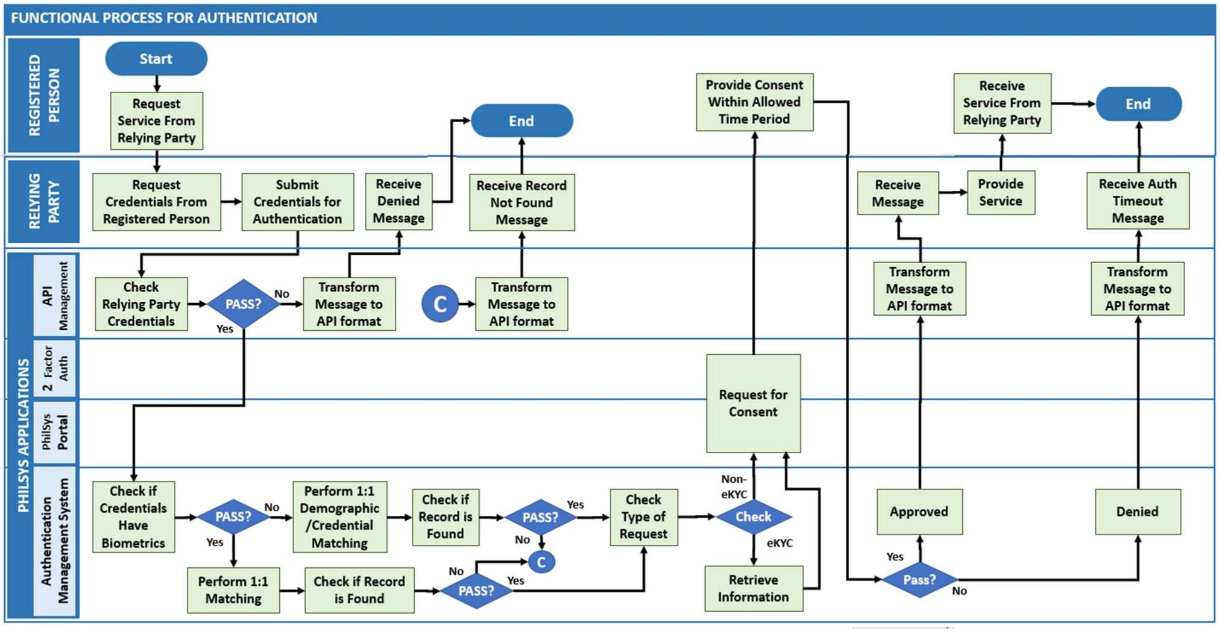
FUNCTIONAL PROCESS FOR AUTHENTICATION
REGISTERED PERSON
RELYING PARTY
PHILSYS APPLICATIONS
API Management
2 Factor Auth
PhilSys Portal
Authentication Management System
Start
Request Service From Relying Party
Request Credentials From Registered Person
Submit Credentials for Authentication
Receive Denied Message
End
Receive Record Not Found Message
Check Relying Party Credentials
PASS?
No
Yes
Transform Message to API format
C
Transform Message to API format
Provide Consent Within Allowed Time Period
Request for Consent
Receive Service From Relying Party
End
Receive Message
Provide Service
Receive Auth Timeout Message
Transform Message to API format
Transform Message to API format
Check if Credentials Have Biometrics
PASS?
No
Yes
Perform 1:1 Demographic /Credential Matching
Check if Record is Found
PASS?
Yes
No
C
Perform 1:1 Matching
Check if Record is Found
No
PASS?
Yes
Check Type of Request
Non-eKYC
Check
eKYC
Retrieve Information
Approved
Yes
Pass?
No
Denied

Figure 10. Authentication Process

The process diagram above shows the underlying processes and dependencies to authenticate a registered person through PhilSys Authentication Services.

a. The process starts where a Registered Person requests for services from a Relying Party (RP).

b. The RP requests for credentials from the Registered Person and submits these credentials to the PhilSys Authentication Services.

c. The RP’s System connects to PhilSys through a ￼public-facing API Management System (APIMS). The APIMS checks whether the RP has the correct system credentials (both Partner and Device credentials) and if the RP is indeed authorized to access the APIs.

d. After the APIMS, the Authentication Management System (AMS) checks if the request contains biometric credentials. If the request indeed contains biometric credentials, the complete Authentication process which includes the following is performed:

1) Data packet decryption

2) Partner Credential

3) Device Credential

4) Demo matching

5) Biometric matching

6) Fraud analytics

e. In order to provide authentication and eKYC service at a high-performance level, the biometric data shall be extracted and stored in the resident data store outside the ABIS. The database licenses and infrastructure (server, storage, etc.) of the resident data store will be provided by the SI. The SI will also be responsible for commissioning and administration, operation and maintenance of the resident data store.

f. The SI shall support the extraction of the templates and shall ensure that resident data store is always in sync with the biometric records in the gallery. The resident data store should be able to support the gallery size and performance levels mentioned in document. The role of BioSP shall be limited to the following:

1) Provide integration support to the SI

2) Ensure quality of extracted templates

g. To serve the biometric authentication request, the authentication solution will utilize the resident data store to extract the relevant biometric and will utilize the Server-Side SDK for matching the stored biometric with the biometric received as part of the request.

h. The integration of authentication application is performed using the middleware products – ESB, BPM and API Gateway. API from different application components would be exposed on the ESB as proxy services which would be leveraged by the BPM engine for orchestration to build composite services to be consumed by UA applications. Authentication extraction being an internal service would not be exposed to outside world and would not be available on the API gateway while eKYC and Authentication would be available on API Gateway.

6.3.6.1.1 Online Authentication: User / Actor: Registered Person

Role: A person registered with the PhilSys and in possession (or issued with) a valid PSN or Alyas PSN.

Table 31. Functional Requirements of Registered Person Access to Service

Functional Requirement	Description
Request to access service (from Relying Party)	The Registered Person MUST be able to request access to a service.
Provide consent within allowed time period	The Registered Person MUST be able to consent to the sharing of personal data requested by a service (Relying Party). Consent MUST be granular and recorded in system logs.

Functional Requirement	Description
Receive access to service (from Relying Party)	The Registered Person MUST be provided with access to the service (pending any service requirements for eligibility) having successfully authenticated against the PhilSys.

6.3.6.1.2 Online Authentication: User / Actor: Relying Party

Role: A service dependent on authentication against the PhilSys registry in order to verify the identity of an individual (Registered Person) when accessing a service.

Table 32. Functional Requirements of Requesting Relying Parties

Functional Requirement	Description
Request for credentials (from Registered Person)	The Relying Party MUST request relevant credentials from the Registered Person in order to authenticate against the PhilSys and thereby gain access to the service.
Submit Credentials for PhilSys Authentication	The Relying Party MUST submit credentials via PhilSys APIs, as developed by the SI, in order to initiate authentication against the PhilSys.
Receive message	The Relying Party MUST be able to receive and act upon the following types of message: • Access denied • Record not found • Successful authentication • Timeout
Provide access to service (for Registered Person)	The Relying Party MUST provide access to the service for a successful authentication (subject to any eligibility checks required by the service).

6.3.6.1.3 Online Authentication: User / Actor: API Management

Role: To provide API services to system components

Table 33. API Management Functional Requirements

Functional Requirement	Description
Check if Relying Party has correct credentials	API Management MUST provide functionality to check that the correct credentials are provided in an API request and that they are in the correct format for processing.
Transform message to API format	API Management MUST provide functionality to format API messages.

6.3.6.1.4 Online Authentication: User / Actor: Two-Factor Authentication

Role: To verify a second factor in addition to PSN where a biometric is not used for authentication and greater certainty is required by the Relying Party that the user is who they claim to be.

Table 34. Functional Requirement of Two-Factor Authentication

Functional Requirement	Description
Check Second-Factor Authentication	The system MUST include functionality to verify a second factor authentication. The nature of the second factor is to be determined by the successful bidder but MUST conform to recognized standards and best practices for secure authentication.

6.3.6.1.5 Online Authentication: User / Actor: PhilSys Portal

Role: Public-facing web portal providing access to registration progress and usage information for applicants and registered users accordingly.

Table 35. Functional Requirement for Request Consent via PhilSys Web Portal

Functional Requirement	Description
Request for consent	The Registered Person MUST be able to consent to the sharing of personal data requested by a service (Relying Party). Consent MUST be granular and recorded in system logs.

6.3.6.1.6 Online Authentication: User / Actor: Central Workflow Engine (CWE)

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

Table 36. Functional Requirements for CWE

Functional Requirement	Description
Check if submitted credentials include biometrics	The CWE MUST include functionality to check that biometrics are included in an authentication request.
Forward 1:1 biometric authentication request to ABAS	The CWE MUST be able to forward the authentication request to ABAS if the packet contains biometric.
Perform 1:1 demographic matching (credentials)	The AMS MUST be able to complete a match between demographic data submitted as part of an authentication request and demographic data associated with the PSN claimed by the Registered Person as part of that authentication.

6.3.6.1.7 Online Authentication: User / Actor: Automated Biometric Authentication System (ABAS)

Role: To provide authentication for a Registered Person against biometric data gathered during registration with the PhilSys Information System.

Table 37. Functional Requirements of ABAS 1:1 Biometric Matching

Functional Requirement	Description
Perform 1:1 biometric matching	The ABAS MUST be able to match biometric data submitted by a registered person during an online authentication attempt against the biometric data held in the PhilSys Registry for the corresponding PSN or Alyas PSN (as declared by the registered person).

6.3.6.2 Offline Authentication

6.3.6.2.1 Offline Authentication: User / Actor: Registered Person

Role: A person registered with the PhilSys and in possession (or issued with) a valid PSN or Alyas PSN.

Table 38. Functional Requirements of Registered Person Access to Service Offline Authentication

Functional Requirement	Description
Request to access service (from Relying Party)	The Registered Person MUST be able to request access to a service when the Relying Party is offline.
Provide proof of identity	The Registered Person MUST be able to show proof of identity using PhilID Card.
Receive access to service (from Relying Party)	The Registered Person MUST be provided with access to the service having successfully provided proof of identity using PhilID Card.

6.3.6.3 Offline Authentication: User / Actor: Relying Party

Role: A service dependent on authentication against the PhilSys registry in order to verify the identity of an individual (Registered Person) when accessing a service.

Table 39. Functional Requirements of Relying Party Offline Authentication

Functional Requirement	Description
Request for credentials (from Registered Person)	The Relying Party MUST request relevant credentials from the Registered Person in order to authenticate using PhilID Card and thereby gain access to the service.
Offline Authentication using PhilID	The Relying Party MUST check the authenticity of the PhilID Card presented by validating the security features of the PhilID card including validation of the digital signature if the QR code is digitally signed. The Relying Party MUST be able to scan the QR Code from the Registered Person's PhilID using a QR Code reader, display QR Code information, and compare the QR Code information with the Registered Person's submitted supporting documents as proof of identity.

Functional Requirement	Description
Provide access to service (for Registered Person)	The Relying Party MUST provide access to the service for a successful offline authentication (subject to any eligibility checks required by the service).

6.3.7 Other PhilSys Services

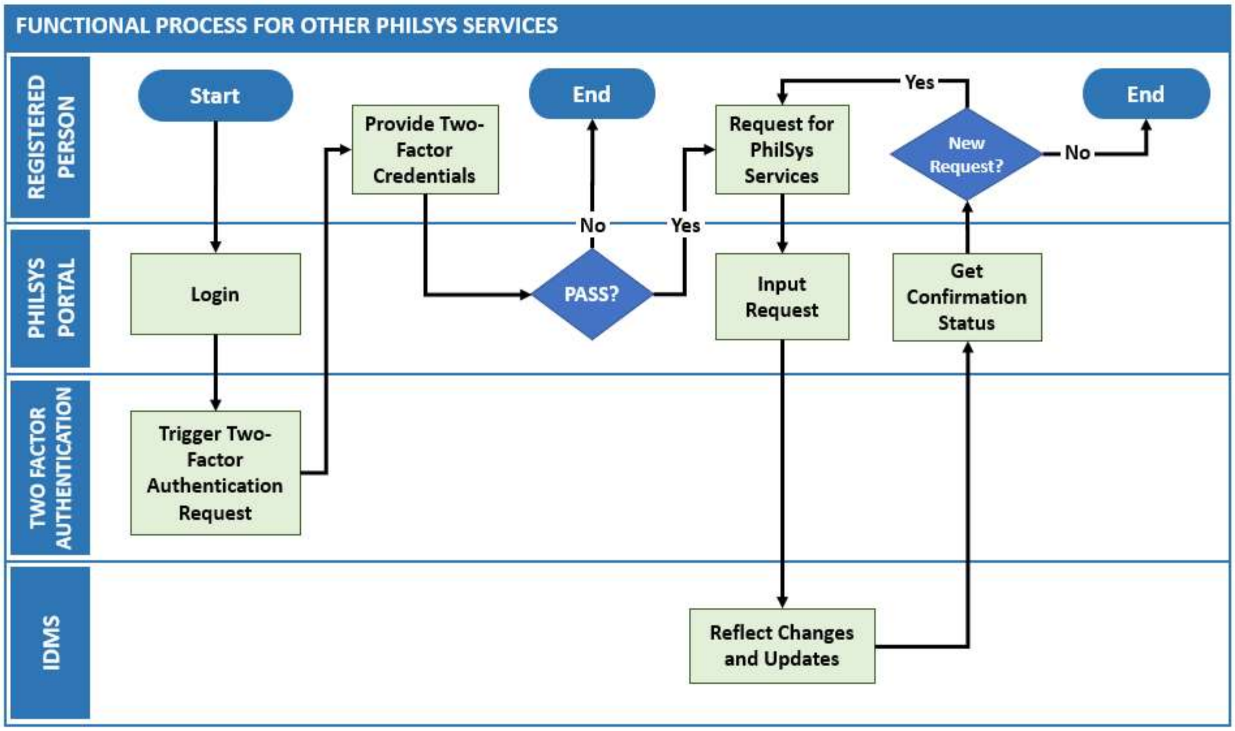
FUNCTIONAL PROCESS FOR OTHER PHILSYS SERVICES
REGISTERED PERSON
PHILSYS PORTAL
TWO FACTOR AUTHENTICATION
IDMS
Start
Login
Trigger Two-Factor Authentication Request
Provide Two-Factor Credentials
PASS?
No
End
Yes
Request for PhilSys Services
Input Request
Reflect Changes and Updates
Get Confirmation Status
New Request?
Yes
No
End

Figure 11. Other PhilSys Services Process

The process diagram above shows the underlying processes and dependencies to facilitate requests for other PhilSys services. Such services include:

a. Update demographic info (Note: configurable by PSA to switch on / off data fields for user updating);

b. Request for card replacement;

c. Review authentication logs and record history;

d. Set permissions for authentication requests;

e. Request for *Alyas* PSN and

f. Portal account management settings.

g. While these services are primarily available online via the PhilSys Portal, it is also available in PhilSys Registration Centers for walk-in requests.

6.4 Detailed Functional Design of PhilSys

The following diagram shows the mapping between PhilSys core business modules and main functions to support:

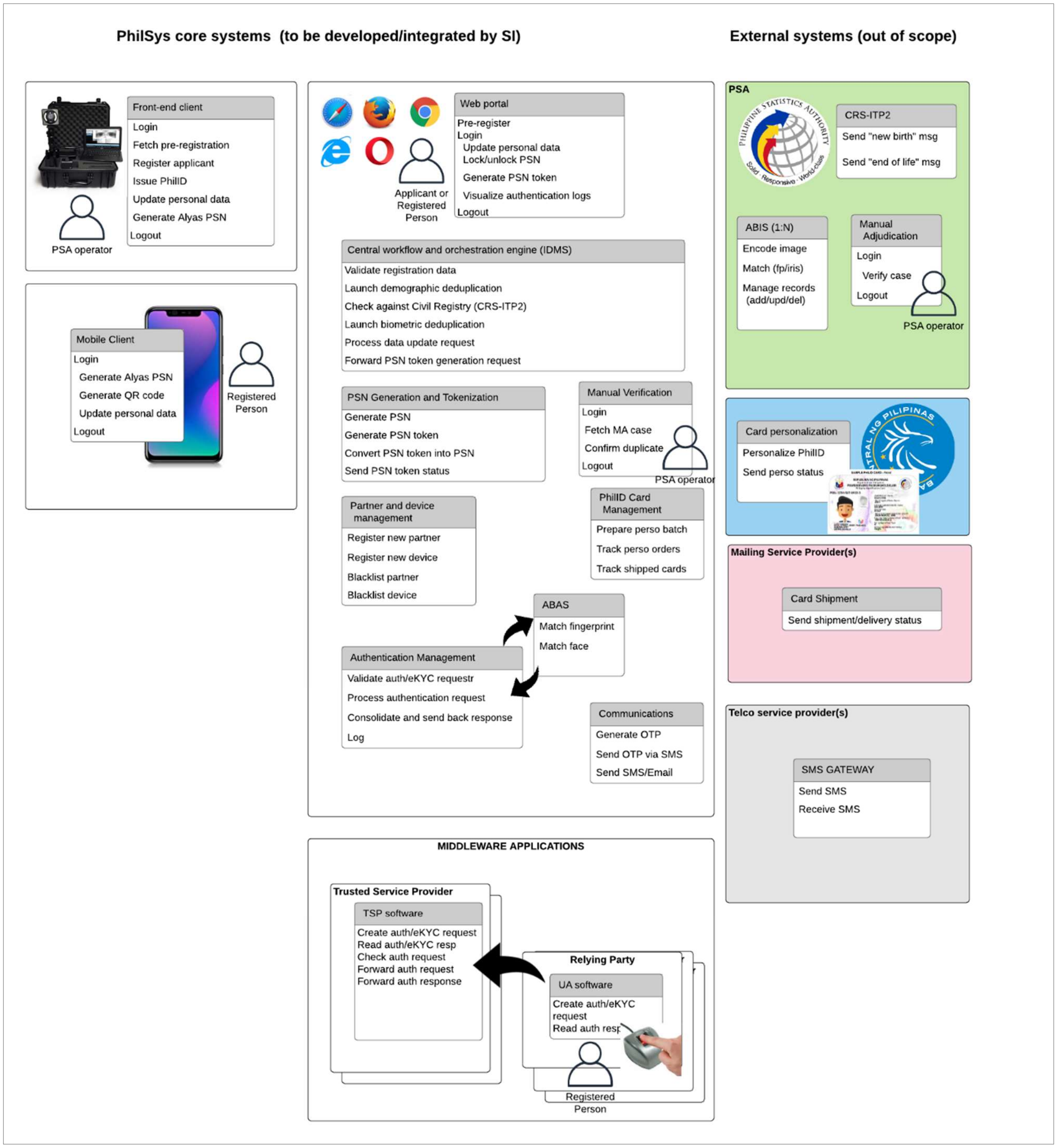

Figure 12. PhilSys Detailed Functional Design

6.4.1 Front-End PhilSys Core Business Systems

6.4.1.1 PhilSys Fixed Registration Center Front-End Client

The PhilSys Fixed Registration Center (PFRC) is also a service channel for walk-in clients to deliver PhilSys services, including registration, credential distribution, data updates, and grievance handling.

The PFRC Front-End Client is the system used in Registration and Fixed / Mobile Registration Centers to access electronic services of PhilSys. All features in this system are accessible only through an authorized PSA user.

The following services or systems are availed at in PhilSys Fixed Registration Centers:

a. Registration Software that provides the following functions:
   1) Login / Logout
   2) Register applicant
   3) Fetch Pre-Registration record
   4) Scan and Upload Supporting documents
   5) Update demographic data (including mobile phone number and e-mail)
   6) Update biometric data
   7) PSN Retrieval / Lost PSN

b. Authentication Services: To authenticate Registered Person who wants to avail of PhilSys services.

c. Other Services
   1) Queueing System that provides the following functions:
      i. Generate queue numbers
      ii. Display queue numbers currently being served
   2) Payment and Billing Solution that provides the following functions:
      i. Verification of payment for card replacement
      ii. Verification of payment for card of resident aliens
   3) Card Management System that provides the following functions:
      i. Request new PhilID
      ii. Card Releasing (through CPMS)
   4) Functions/services available in PhilSys Web Portal and PhilSys Mobile Application.

6.4.1.1.1 <u>Registration Software</u>

6.4.1.1.1.1 Facilitate Registration Process

The Registration Client must enable the Applicant, via the PSA operator, to submit and process the needed data for registration. The Front-end must log all relevant information and metadata as prescribed by the Record History[3]. Moreover, the Registration Client must be able to print a Transaction Reference Number as confirmation for the Applicant that the information submitted are confirmed accurate and complete.

6.4.1.1.1.2 Fetch Pre-Registration Data (Online)

If the Applicant submitted partial data via pre-registration, the information submitted to the PhilSys Portal must be downloaded to the Registration Client on or before the set appointment date and on the right Registration Center. The Registration Client must be able to link-match the downloaded information with the Transaction Reference Number issued during the Pre-Registration via the PhilSys Portal. Fetching Pre-Registration Data can only be activated for Registration Clients in Registration Centers with stable network connectivity.

6.4.1.1.1.3 Facilitate Updating of Registered Person's Personal Data (￼￼Demographic and Biometric)

The Registration Client must be able to facilitate updating of a Registered Person's Personal Data, including biometric and demographic updates. This update is done through a PSA operator.

6.4.1.1.2 <u>Other Services – PhilSys Fixed Registration Center</u>

6.4.1.1.2.1 Facilitate Request for Registered Person's Reissuance of PhilID

The PhilSys Fixed Registration Centers must be able to facilitate the request for the reissuance of the Registered Person's PhilID. This feature must integrate with a Payment Gateway to facilitate requests needing payments.

[3] See RA 11055 Definition of Record History

6.4.1.1.2.2 Facilitate Generation of Alyas PSNs

The PhilSys Fixed Registration Centers must facilitate the generation of the *Alyas* PSN upon the request of the Registered Person. The Registered Person, through the PSA operator, may choose the valid duration of the *Alyas* PSN and request for a printout to confirm that the token was generated. Because the generation of the *Alyas* PSN are done centrally, activating this feature in the PhilSys Fixed Registration Center will need to have stable network connection to PSA Central Servers. *Alyas* PSN and its generation must comply with guidelines that will be set by the PSA.

The registered person can have multiple active Alyas PSN.

6.4.1.1.2.3 Facilitate Setting of Permissions for Authentication Requests

The PhilSys Fixed Registration Centers, through the PSA operator, must facilitate the setting of permissions for authentication requests. This feature enables the Registered Person to allow or deny, either in full or in partial, any authentication requests coming from Relying Parties. To use this feature, the PhilSys Fixed Registration Center will need to have stable network connection to the PhilSys Registry. Changes in the authentication permission settings shall form part of the Record History.

6.4.1.1.2.4 facilitate authentication of registered person.

The PhilSys Fixed Registration Center must facilitate the online biometric authentication of Registered Persons. For this feature, the PhilSys Fixed Registration Center will need to have stable network connection to PSA Central Servers. Approval or disapproval of authentication requests shall form part of the Record History. This may be used to authenticate persons during PhilID card issuance.

6.4.1.1.2.5 Facilitate Submission of complaints

The PhilSys Fixed Registration Center must facilitate the submission of complaints from Applicants and Registered Persons, using the Transaction Number and the PSN or *Alyas* PSN respectively. This feature allows the complainant, via the PSA operator, to submit, track, and review the responses to the complaints submitted. For this feature, the PhilSys Fixed Registration Center will need to have stable network connection to PSA Central Servers to accommodate grievance and complaints.

6.4.1.1.2.6 Queueing System

The Queueing System is an automated system designed to manage walk-in services, or customer flow at the PhilSys Fixed Registration Center. The Queueing System has the following features:

i. Select Transaction Type and Generate Queue Number.
ii. Display current serving queue numbers at the digital signage system.
iii. The clients are called and directed to the service counter by the digital signage system. The calling is done via a software installed at the service counter's system.

6.4.1.1.2.7 Payment and Billing Solutions (PBS)

The Payment and Billing Solutions is designed to allow various stakeholders and residents to make payments for PhilSys services. The PBS captures the purpose of payment, details of the user and calculates fees based on configurable business rules. The PBS is used for transactions such as Card Replacement and Resident Alien Application involving payments.

6.4.1.2 PhilSys Web Portal

6.4.1.2.1 Pre-Registration

The PhilSys Web Portal will provide applicants with the ability to complete a pre-registration process gathering demographic data as required by the registration process. Pre-registration applicants will also have the option to upload documents required by the registration process and required to select a PhilSys Fixed Registration Center and appointment timeslot for completion of the registration process.

The PhilSys Web Portal will also provide pre-registration applicants with an *Appointment Reference Number* which will be subsequently used by Registration Officers to complete the registration process at a PhilSys Fixed Registration Center (requiring internet connectivity at the Center). Acknowledgement of the pre-registration, including the appointment reference number, appointment time-slot details, and selected PhilSys Fixed Registration Centers, will be provided to the Applicant for printing.

6.4.1.2.2 Viewing Progress of Registration

Applicants who have recently completed registration at a PhilSys Fixed Registration Center or PhilSys Mobile Registration Center may wish to view the progress of their application. The PhilSys Web Portal will allow these individuals to view the progress of their application by entering their Registration Transaction Number (issued after completing their registration) and the date of birth they provided at registration. The information displayed by the portal should not include any demographic data other than the name that the applicant provided at registration alongside an indication of progress against the application (e.g. Card in Production).

6.4.1.2.3 Account Creation and Authentication on PhilSys Web Portal

a. Other than viewing public information (such as service updates and guidance), all users will need to authenticate before accessing functionality where personal or sensitive data can be viewed or updated.

b. Registered Persons visiting the PhilSys Web Portal for the first time will be required to create a PhilSys Web Portal specific account for logging into the PhilSys Web Portal. To do so, Registered Persons must provide their PSN and the date of birth provided at the time of registration to request a new account. If the PSN does not have an account already created against it, a One Time Password (OTP) will be sent to the mobile number and / or email account provided by the registered person at the time of registration and a request made in the PhilSys Web Portal for the OTP code to be entered. If successful, the user will be able to create a new PhilSys Web Portal account, including the creation of a password for subsequent sign-on.

c. Authentication through the PhilSys Web Portal (post account creation) will require individuals to provide either their PSN or PCN and password which will then result in an OTP code being sent to their registered mobile number and / or email account (i.e. multi-factor authentication). On successful entry of the OTP code, access will be granted to the Web Portal. All data updates through the Web Portal will require an additional successful OTP authentication.

d. The PhilSys Web Portal will also provide the ability for passwords to be recovered using the registered person's PSN or PCN, date of birth and a successful OTP authentication. After a certain number of attempts, the PhilSys Web Portal account will be locked and can only be unlocked by the registered person visiting a PhilSys Fixed Registration Center.

e. All attempted logins and transactions on the PhilSys Web Portal will trigger a notification by SMS and / or e-mail (if these have been provided by the registered person).

6.4.1.2.4 View or Update Demographic Data

a. Registered persons wishing to view demographic data recorded as part of their PhilSys record may do so by accessing the PhilSys Web Portal authenticating themselves with their PhilSys account and password

b. The Registered Person may update his/her demographic data as part of their PhilSys record after a successful OTP authentication.

c. Once authenticated, Registered Persons will be able to change selected demographic data if they so wish and submit these changes to the PhilSys Registry System for processing.

6.4.1.2.5 View Record History and Select Preferences for Retention Period

a. Registered persons wishing to review their record history, as prescribed by the Philippines Identification System or RA 11055 may do so by accessing the PhilSys Web Portal authenticating themselves with their PhilSys account, password and an OTP authentication as described above.

b. The record history will be presented in a user-friendly and easy-to-understand format.

c. Once authenticated, registered persons will be able to adjust the period for which transactions associated with their PhilSys record are viewable. Registered persons will be able to report suspicious transactions to the Contact Center.

6.4.1.2.6 Locking / Unlocking Authentication for PSN

a. Registered persons wishing to lock and unlock their PSN (for authentications), may do so by accessing the PhilSys Web Portal authenticating themselves with their PhilSys account, password and an OTP authentication as described above.

b. Once authenticated, registered persons will be able to lock or unlock their PSN (preventing authentications), including to set a time period (in hours or days) for their PSN to be locked.

6.4.1.2.7 Generation of the Alyas PSN

Registered persons wishing to generate an *Alyas* PSN (a temporary token of their PSN, used to hide the PSN and PhilSys Card Number for transactions), may do so by accessing the PhilSys Web Portal authenticating themselves with their PhilSys account, password and an OTP authentication as described above. Once authenticated, registered persons will be able to generate the *Alyas* PSN.

6.4.1.2.8 Request for a new PhilID Card

Functionality should be provided for registered individuals authenticated through the PhilSys Web Portal to request a new PhilID Card. A reason for reissue should be provided by the individual and proof of payment before a new card can be issued.

6.4.1.2.9 Report of Lost / Stolen and Damaged PhilID Card

Registered individuals authenticated to the PhilSys Web Portal must have the ability to report lost or stolen PhilID Cards. This should result in the issuance of a new card (if requested by the individual) and must be recorded in order to invalidate lost or stolen cards (lock PCN) with regards to authentication.

6.4.1.3 PhilSys Mobile Application

The PhilSys Mobile Application (PMA) is the system used by a Registered Person to access PhilSys services through mobile application capable devices. The Mobile Application would require regular network connectivity to PSA Servers for periodic synchronization of data, security patches, and online-only PhilSys services. The PhilSys Mobile Application is centrally managed by PSA and is published in common mobile application stores, free of charge to the user. The PMA must allow selection of data items that can be updated based on PSA policies.

6.4.1.3.1 User Login and Logout

Before any access to the internal features are permitted, the PhilSys Mobile Application must recognize Registered Persons that enabled access via the Mobile Application, Users must enable the PhilSys Mobile Application through two options: (i) via the Front-end Registration in PhilSys Fixed Registration Centers or (ii) via the PhilSys Web Portal. Login action involves the user to input their username and password. The PhilSys Mobile Application must be capable of user-opted logout and automated logout due to system time out.

6.4.1.3.2 Manage Alyas PSNs

The Mobile Application MUST allow a registered person to generate and manage (i.e. display/deactivate/activate/delete) multiple concurrent and active Alyas PSNs. For each Alyas PSN, the Registered Person may choose the validity period as well as the personal data that can be shared by the PhilSys when using the same Alyas PSN in the frame of an online eKYC request. Because the generation of the Alyas PSNs is done centrally, activating this feature of the PhilSys Mobile Application will need to have stable network connection to PSA Central Servers. Alyas PSNs and their generation must comply with guidelines that will be set by PSA.

6.4.1.3.3 Generate QR Code

The PhilSys Mobile Application must be able to generate a QR Code (with embedded machine readable Alyas PSN) upon the request of the Registered Person. QR code can also be generated for active *Alyas* PSN at any point in time. In the latter case, the QR must embed validity period and list of personal data that can be shared by the PhilSys Registry in the frame of an online eKYC request. The Registered Person may request for an electronic document that can be downloaded or shared to the user's device or email. QR Code and its generation must comply with guidelines that will be set by PSA including digital signing and encryption which are already provided as features in MOSIP.

6.4.1.3.4 Generate virtual Phil ID Card image

The PhilSys Mobile Application must be able to generate and display a virtual PhilID card (simple image) that complies with the final design of the PhilID Card.

Update Personal Data (Demographic)

The PhilSys Mobile Application must be able to update a Registered Person’s Demographic Data4. This update requires the Registered Person to be authenticated first with the PhilSys Registry before any updates are made. Data updates and metadata shall form part of the Record History.

6.4.1.3.5 Request for Reissuance of PhilID

The PhilSys Mobile Application must be able to facilitate the request for the Registered Person’s reissuance of their PhilID. This feature of the Mobile Application must be integratable with a Payment Gateway[5] to facilitate requests needing payments[6].

6.4.1.3.6 Setting of Permissions for Authentication Requests

The PhilSys Mobile Application must have a feature to allow the user to configure the permissions for authentication requests. This feature allows the Registered Person to allow or deny, either in full or in partial, any authentication requests coming from Relying Parties. Activating this feature of the PhilSys Mobile Application will require stable network connection to PhilSys Registry. Changes in the authentication permission settings shall form part of the Record History.

6.4.1.3.7 Submit Complaints

The PhilSys Mobile Application must have a feature for the submission of complaints from Applicants and Registered Persons, using the Transaction Number and *Alyas* PSN respectively. This feature allows the complainant to submit, track, and review the responses to the complaints submitted. Activating this feature of the PhilSys Mobile Application will need to have stable network connection to PhilSys Registry.

6.4.1.3.8 View Record History

The PhilSys Mobile Application must enable the user to view his / her Record History. The system must also enable the user to manage the duration of how long the Record History should be viewable in the PhilSys Registry. This feature shall use basic data visualizations over registration and authentication with the option to generate the records in tabular format. Registered Persons are permitted to forward their Record History to their chosen email address.

[4] Subject to PSA/PhilSys Guidelines on updating data via Mobile Application

[5] To be jointly identified by PSA/PhilSys and DOF

[6] Guidelines to be issued by PSA/PhilSys

6.4.1.3.9 Summary of PMA

Table 40. Functional Requirements of PhilSys Mobile Application

#	Requirement	Business / Functional Requirement Description
1. Access Management and Registration		
a.	Login	The resident should be able to login to the mobile application to access secure features.
b.	Security Level	The security controls are defined at the functionality level.
c.	Registration	No registration would be required for accessing the mobile application. However, certain services would require the resident to have a PSN number.
2. Portal Features		
a.	Language	**The mobile application should be viewed in English, and Filipino.**
b.	Home Page	The home page should provide details and links of services which the resident can avail on the mobile application
3. Services		
a.	Registration Centers information	The application should utilize location services of mobile to detect users' location and show nearby registration centers. Alternatively, the user should also have the option to select a location (region, province / prefecture, etc.). After selecting this location, an area and result should be shown on map with distance, directions, address, and contact numbers of the center.
b.	Pre-registration	The resident should be able to open the pre-registration web application from the web application in the mobile's browser.
c.	PSN Status	The resident should be able to check his PSN status post registration using Transaction Reference Number (TRN).
d.	Download PSN	The application should allow a resident to download a PSN card using the PSN number and OTP authentication. The resident would enter his PSN number on the screen followed by an OTP based authentication. Successful authentication would allow the PSN to be downloaded as a secure PDF.
e.	Get PSN on mobile	The application should allow a resident to receive PSN on mobile number and OTP authentication. The IDMS should search the identity repository for given mobile number. In case the mobile number exists in the record for some PSN as a registered mobile number, an OTP should be sent to the mobile number for

#	Requirement	Business / Functional Requirement Description
		authentication. The resident would enter his mobile number on the screen followed by an OTP based authentication. Successful authentication would allow the PSN to be received as an SMS on the registered mobile number.
f.	Retrieve Lost TRN	The application should allow the resident to retrieve lost TRN by entering the demographic details such as Name, Gender, Date of Birth and Mobile Number.
g.	Retrieve Lost PSN	The application should allow the resident to retrieve lost PSN by entering the demographic details such as TRN (optional), Name, Gender, Date of Birth and Mobile Number.
h.	PSN information update	The application should direct the user to the web portal where this functionality is available.
i.	Verify PSN	The application should allow anyone to enter the PSN number for which the details are required. After an OTP authentication, the application should be able to show basic details such as: • Gender • Broad Age Group (e.g. 30 – 40 years) • Region or Province The exact details to be displayed after OTP verification may be decided at the time of implementation. This “Verify PSN” service could be offered as a separate, standalone web service published on the internet.
j.	Verify Mobile / Email Address	The application should allow anyone to enter the PSN number for which the mobile number and email address are to be verified. The application should ask for the PSN and show masked Mobile Number and Email Address. Alternatively, the application should ask resident to enter the mobile number and / or email address and verify whether the details match its record or not.
k.	Lock / Unlock Biometrics	The residents may want to secure their authentication by locking their biometrics and unlocking them only when required. The application should allow the resident to enter the PSN. The application should send the OTP to the mobile number registered with it for the given PSN. The application should allow the resident to enter OTP or read it automatically from SMS directory. Upon submission of PSN, the application should verify the same. After

#	Requirement	Business / Functional Requirement Description
		due verification, the application should allow the resident to lock / unlock the biometrics for: • A given time period, or • Till further lock / unlock For the given PSN, this should immediately impact all the functionalities in the PhilSys Information System. Moreover, the communication should be sent to the resident about the locking / unlocking of biometrics.
l.	PSN Authentication History	The application should direct the user to the web portal where this functionality is available.
m.	Grievance Logging and Status	The application should direct the user to the web portal where these functionalities should be available.
4. Management of Alyas PSNs		
a.	Generate Alyas PSN	The application should have the provision to generate an Alyas PSN taking PSN and OTP as an input.
b.	Display active and Deactivated Alyas PSNs	This application should have the provision to display all active and deactivated Alyas PSNs for the resident by taking the PSN and OTP as an input.

6.4.2 Backend PhilSys System

6.4.2.1 IDMS

A registration packet is received in the IDMS and process it in a sequential staged manner from the validation of the packet to the generation of PSN and intimation of the PhilID to the resident. This application shall contain a management and a core layer. The management layer will orchestrate requests and the core layer will host the business logic. This system shall execute the following steps in a stage-wise manner through an orchestration middleware:

- Ensuring structural integrity of the transmitted information along with other validations.
- Perform a demographic de-duplication operation wherein any duplicates are identified based on demographic details.
- Coordinate a biometric deduplication operation with the Automated Biometric Information System (ABIS) to perform a biometric deduplication check for the registration packet.

- Generate PSN using a Generator, which will be placed outside the IDMS and would be used for generating PSN and Tokens.
- Coordinate with SMS/Email system for sending the PSN number to the resident
- Coordinate with printing agency.

6.4.2.1.1 Validate Registration Data

The IDMS validates registration data and metadata contained in all incoming Registration packets, including integrity, completeness, format validation, timestamping and presence of malware / viruses. It also checks the validity of the Registration device as well as the Registration operator by interfacing with the PDMS. In case of an exception during the validation, the IDMS creates and queues a new case for manual verification. Upon successful validation, the IDMS logs the Registration metadata and store the business data in the designated data store. The IDMS also checks the quality of the biometric data (portrait photo, iris and fingerprints) using SDKs that will be provided by the biometric vendor.

6.4.2.1.2 Launch Demographic Deduplication

The IDMS compares each set of demographic data against the PhilSys Registry. It carries out an automated demographic deduplication by matching all demographic fields against PhilSys Registry records. In case of duplicates, the IDMS raises an exception.

6.4.2.1.3 Launch Biometric Deduplication

The IDMS initiates an automated biometric deduplication by interfacing with the ABIS that will be provided by the biometric vendor. The IDMS generates and sends a biometric or multi-biometric 1: N request (containing IDMS transaction number and biometrics) to the ABIS. The ABIS will pull the data relating to the 1: N request from the IDMS. Each biometric deduplication is done against all PSN holders.

The IDMS receives and stores ABIS output and generates PSN.

6.4.2.2 Document Management System

The Document Management System gets and stores accompanying documents of each registration record in a dedicated storage. The documents are linked to the assigned PSN.

The Registration Officer will have to scan registration forms and accompanying documents tagged with Transaction Reference Number (TRN) from registration centers. The documents have to be systematically scanned. The scanned documents should have at least 600 dpi.

Scanning facility of forms and documents will have to be provided with due quality checks (scanned image should not be blurred, folded, too dark or too light to read etc.). Scanned image of the document should be clear and readable. Photo of resident should be identifiable. Scanned data will be linked with Transaction Reference Number for ease of retrieval.

The following are minimum functions of the DMS:

a. Manage access to uploaded supporting registration documents
b. Store registration forms and supporting documents
c. Store, search, retrieve, display and share PhilSys internal documents

6.4.2.3 Manual Verification

If the ABIS cannot conclusively identify a unique record or if the FDMS raises an alarm, the applicant's record undergoes a manual verification process. Manual verification involves PhilSys Officers manually reviewing potential duplicates or fraud and deciding on the application request either by: (i) approving the application due to false positives or (ii) forwarding for further investigation.

6.4.2.3.1 User Login and Logout

The Manual Verification System must recognize legitimate PSA users before any access to the internal features are permitted. Login action involves the user to input their username, password, and biometrics or FIDO dongle before access to the system is granted. The user credentials must be pre-loaded centrally before the Manual Verification are deployed. The Manual Verification System must be capable of user-opted logout and automated logout due to system time out.

6.4.2.3.2 Fetch Manual Verification Case

During Manual Verification, the system displays the demographic information of transaction record with possible match in the PhilSys Registry, at this stage, the PSA operator may fetch the corresponding Manual Adjudication results to help in the resolution of the status of the current transaction record.

6.4.2.3.3 Confirm Duplicate

If the PSA operator confirms that the current transaction record is a duplicate of an existing PhilSys Registry record, the Manual Verification System shall flag the Registration request as "Duplicate".

6.4.2.3.4 Disconfirm Duplicate

Records that are tagged as “Duplicate” may undergo Final Verification. A PSA officer may perform further review of the manual verification results. If the review determines that the transaction record is not a duplicate, the PSA officer shall disconfirm the duplicate.

6.4.2.4 PSN Generation and Tokenization Management System (PSNGTMS)

The PSNGTMS must support the generation and management of PSNs as well as all types of PSN tokens mentioned in Section 6.2.2.

6.4.2.4.1 Management of “root” PSNs and PCNs

After a successful biometric deduplication, the PhilSys must generate a 12-digit PSN and a 16-digit PSN token called the PhilSys Card Number (PCN). Whenever a PhilID card is declared lost or stolen, the PhilSys must de-activate the corresponding PCN: the latter cannot be used in the frame of an authentication or eKYC transaction.

6.4.2.4.2 Management of Alyas PSNs

Upon registered user’s demand The PhilSys will generate a new 16-digit Alyas PSN at the request of a registered user. Contrary to “root” PSNs and PCNs, multiple Alyas PSNs can co-exist for the same registered user

6.4.2.4.3 Management of PSN tokens for the seeding of stable PSN at a relying party (privacy preserving vertical PSN seeding)

Upon the signature of an agreement with a given onboarded relying party, the PhilSys must support the management of “back-end” PSN tokens (linkage and dissemination): each time the PhilSys processes an authentication/eKYC transaction emanating from this relying party, if a PCN or Alyas PSN token is used, the PhilSys must append a “stable, back-end” PSN token to the response sent back to the relying party.

6.4.2.4.4 Management of PSN tokens for interoperability (privacy-preserving horizontal PSN seeding)

Upon the signature of a data sharing agreement between two or more onboarded relying parties, the PhilSys must allow to manually configure an interoperability service in order to disseminate common PSN tokens among those parties.

6.4.2.4.5 Management of technical internal PSN tokens

The PhilSys (via the PSNGTMS) must also be able to manage internal PSN tokens in order to hide the "root" PSNs from subsystems such as the external ABIS.

6.4.2.5 PhilID Card Management

A Card Production System (CPS) is to be provided by Bangko Sentral ng Pilipinas (BSP). The CPMS will be deployed to both card production and card personalization facilities. The production and personalization process will be in BSP East Avenue Complex, Quezon City.

The CPMS to be used by PSA will be integrated to the PhilSys Information System, and it will be the role of the SI to publish the API to be used by the Card Production Team stationed at BSP.

6.4.2.5.1 Prepare Personalization Batch

a. Card production is a two-step process. BSP is responsible in the production of blank cards using their own printing machines. PSA is responsible for personalization of the cards using a different set of printing machines.

b. The card production and card personalization processes are physically separate from each other. Cards produced by BSP will be turned over to PSA for personalization.

.

6.4.2.5.2 Generate Print Files for Card Personalization

a. The CBU generates print files containing PCN, demographic information, front-facing photograph and QR Code (with embedded metadata) of records for card printing.

b. The QR code contains the registered person's PCN, name and other demographic information, and two best fingerprints' labels.

c. The CBU groups print files into batches of card production request packets and forwards these to the CPMS.

6.4.2.5.3 Track Personalization Orders

a. The PSA shall track and perform Quality Assurance Testing for all orders for card personalization.

b. The SI shall provide a system for tracking and monitoring the delivery of all PhilID cards.

c. The SI shall integrate the system for tracking and monitoring of PhilID cards to integrate to PhilSys Web Portal and Mobile Applications.

6.4.2.6 Partner and Device Management (PDMS)

Partner and Device Management involves registration or blacklisting authentication/registration partners and devices. Actions performed by PSA operator using PDMS shall be based on approved memo from PSA.

6.4.2.6.1 Register New Partner

Once a new partner has been approved by PSA, the PhilSys shall assign the new partner a unique Partner Code. Partner details such as name, address, contact information, and transaction types allowed (e.g. Registration, Authentication) shall be entered into the system. The system shall automatically generate licenses and keys for the new partner.

6.4.2.6.2 Register New Device

Once new devices for authentication (e.g., fingerprint scanner, iris scanner) have passed PhilSys compliance testing, the PSA operator shall register these devices into the system including device details such as serial number, product ID, device type, location, partner code, etc.

6.4.2.6.3 Blacklist Partner

Once the partner has been blacklisted by PSA, PSA operator will block/deactivate the account and will enter reasons for blacklisting. The PDMS will tag the registered partner as blacklisted along with all devices associated with the blacklisted partner.

6.4.2.6.4 Blacklist Device

Once a device has been identified by PSA for blacklisting for reasons related to security or quality of data submissions to PhilSys or non-conformance to PhilSys standards, PSA Operator will block / deactivate the device and will input reasons for blacklisting. The PDMS will tag the registered device as blacklisted with its corresponding device details such as serial numbers, product ID, device type, location, partner code, etc.

6.4.2.7 Authentication Management System (AMS)

The SI MUST customize, test, install and maintain the Authentication Management System (AMS) that will receive the authentication requests originating from RPs and routed through the Trusted Service Providers (TSPs), process them and send back the authentication result to the requesting TSP.

6.4.2.7.1 Process Authentication / eKYC Request

a. For each incoming authentication or eKYC request, the Authentication Management System (AMS) will check its validity by decrypting and checking packet security, checking data validity, and validating source by integration with PDMS.

b. When the AMS receives a biometric-based authentication request, the system forwards the request to the Automated Biometric Authentication System (ABAS) to perform a 1:1 biometric matching.

c. If the submitted credentials are non-biometric in nature, the system performs 1:1 demographic or credentials matching.

6.4.2.7.2 Process authentication / eKYC Response

a. Once the request has been validated, the AMS will check the authorization by validating the PSN or *Alyas* PSN, and the confirmation that the Registered Person permits the sharing of his / her demographic details.

b. Requests that are tagged as authorized by the AMS will proceed to the authentication process as follows:

   1) Verify the request type;

      The AMS checks for the type of request (i.e. Simple Authentication or eKYC). If the request is eKYC, an additional step to retrieve the requested data is performed. Afterwards, a two-factor authentication challenge or a confirmation via the PhilSys Web Portal will be sent to the registered person and wait for his / her consent. If consent is not given in the allowed timeframe, the AMS forwards an authentication timeout message to the Relying Party. If consent was given in the allowed time frame, the AMS forwards an authentication response appropriate to the authentication request submitted.

   2) Dispatch the request(s) to the concerned authentication subsystem;

   3) Consolidate results received from the concerned authentication subsystem(s);

   4) Sign, encrypt and send consolidated result to the requesting registration; and

   5) Send a notification via SMS (if phone number is registered) as well as the result of the authentication.

6.4.2.7.3 Log Transaction

The AMS shall log all details related to the processing of Authentication requests.

6.4.2.8 Automated Biometric Authentication Services (ABAS)

The ABAS processes requests to authenticate individuals against fingerprints, irises or facial images stored by the PhilSys Registry.

6.4.2.8.1 Match (Fingerprint / Iris / Face)

If an authentication request coming from a Relying Party contains biometrics, ABAS uses the *Alyas* PSN to retrieve biometric templates from the PhilSys Registry and performs 1:1 biometric matching. If there is a match, the system responds with YES and provides requested information. Otherwise, the system responds with NO. ABAS creates logs related to the authentication requests and stores them into the PhilSys Logs.

6.4.2.8.2 Manage Records (Add / Update / Delete)

a. The SI MUST design, develop, test, install, integrate with all relevant PhilSys systems and maintain the following data stores.

b. The data stores can come under the form of a database or rely on a file system, this is left to the appreciation of the SI as long as they do not become bottlenecks and allow to meet SLA requirements.

   1) Pre-registration records

      The SI MUST design, develop, install and maintain a data store for storing all data uploaded by applicants via the pre-registration website.

   2) Registration records

      The SI MUST design, develop, install and maintain a data store for temporarily storing the registration records received from the Registration Software and managed by the IDMS. The SI MUST integrate this data store with the systems that manage the following items:

      a. Scanned Supporting documents

         The SI MUST design, develop, install and maintain a data store for the scanned copy of accompanying documents submitted during registration and personal data update. The SI MUST integrate this data store with the following system(s): DMS.

      b. PSN and PSN tokens

         The SI MUST design, develop, install and maintain a data store for storing all PSNs and PSN tokens generated, including correspondence tables. The SI MUST integrate this data store with the following system(s): PSNGTMS. The SI MUST ensure the highest level of security by using strong encryption.

c. PhilID card status

   The SI MUST design, develop, install and maintain a data store for storing the lifecycle status of all PhilID cards. The SI MUST integrate this data store with the following system(s): CMS.

d. Data store of individuals

   The SI MUST design, develop, test, install and maintain the "data store of individuals" that will be used by the AMS to proceed to authentications. This data store of individuals MUST contain the following data:

   i. Full set of demographic data

   ii. Portrait photos

   iii. Fingerprint images in JPEG2000 Lossless compression

   iv. Fingerprint templates in standard ISO format

   v. Iris images in JPEG2000 format

e. PhilSys logs

   The SI MUST design, develop, install and maintain a data store for storing all logs generated by all PhilSys systems.

6.4.2.9 Notification System (NS)

The SI will design, develop / customize, test, install and maintain the Notification System that manages communication between the PhilSys and the registered persons / clients such as OTP request, Verify OTP request, SMS, and Email notification.

6.4.2.9.1 Generate OTP

If there is a request for OTP generation from the Authentication and Registration APIs, the Notification System will verify if the request is registered and authorized to connect to PhilSys platform. Once verified the Notification System will generate an OTP with a validity period.

6.4.2.9.2 Send OTP via SMS

The generated OTP with a validity period will be sent to the corresponding Registered Person's mobile number.

6.4.2.9.3 Send OTP via Email

The generated OTP with a validity period will be sent to the corresponding Registered Person's Email.

6.4.2.9.4 Send SMS / Email

Any transaction or request for OTP through the PhilSys Platform will be automatically forwarded to the Registered Person's corresponding Mobile number or Email. Logs shall be generated for this transaction or request and stored into the PhilSys Logs.

6.4.2.9.5 Verify OTP

The system verifies the submitted OTP and returns confirmation or rejection of the OTP authentication to the requesting party.

6.4.3 Back-End PhilSys Support Systems

6.4.3.1 Fraud Detection and Management System (FDMS)

The Fraud Detection and Management System shall analyze and monitor all business and technical transactions processed by the PhilSys and detect potentially fraudulent cases and either block transactions or allow PSA operators to investigate the same.

The SI shall provide an FDMS that will allow real-time and non-real time fraud detection functionalities. The FDMS shall allow PSA operators to detect potentially fraudulent cases and either block such transactions or initiate more in-depth investigations.

6.4.3.1.1 Parse PhilSys Logs

Parse logs to enable real-time and non-real time fraud detection both for authentication and registration including logs of manual adjudication and manual verification.

6.4.3.1.2 Tag Cases as Abnormal Registration

Tag as abnormal for multiple registrations from same PSA operator or registration kit or same fixed registration center. Tag as abnormal for registrations outside of normal business hours.

6.4.3.1.3 Tag Cases as Abnormal Authentication

Tag as abnormal for authentication patterns such suspicious behaviors, repeated attempts or operations outside of normal business hours or from same authentication device or same Relying Party.

6.4.3.1.4 Tag Cases for Automatic Blocking

Tag for automatic blocking registration or authentication transactions classified as suspicious behaviors (to be defined later by PSA).

6.4.3.1.5 Forward Fraud-Tagged Cases for Investigation
Forward cases identified as possible fraud to investigation. IVID shall perform actual investigation process.

6.4.3.1.6 Generate Reports
Generate reports on cases that are tagged as fraudulent.

6.4.3.2 Business Intelligence and Analytics System (BIAS)

Configurable analytics software will be required to analyze data and logs gathered from services, access management systems, operational monitoring and other sources (e.g. relying party and fulfilment services logs as required). This will allow PSA to report and monitor service performance and operation in a clear, timely and queryable interface.

The analytics software would be a separate system and does not need to be directly integrated with the wider PhilSys Registry and its subsystems. The ability to consume data/log feeds in multiple text-based formats and to automate the collection and processing of feeds must be included.

The SI shall provide BIAS with the following minimum functionalities:

6.4.3.2.1 Generate data analytics
BIAS automatically generates analytics from PhilSys logs and data.

6.4.3.2.2 Update Dashboard
BIAS automatically updates the management and operational contents of the dashboard to enable PSA to monitor PhilSys operations

6.4.3.2.3 Generate Scheduled Reports
BIAS generates scheduled reports based on PSA requirements

6.4.3.2.4 Provide Ad-Hoc Queries

BIAS provides functionality to create ad-hoc queries.

6.4.3.3 Customer Relationship Management System (CRMS)

a. For complaints by members of the public as well as PSA partners, PSA operators/staff records all incidents and complaints in CRMS and track them using dedicated unique identifiers. The CRMS timestamps all transactions and automatically prioritize them based on the distance with the relevant KPIs of the SLA. The CRMS also keeps a history of all transactions not limited to metadata, but including identifiers, timestamps and content of all exchanges.

b. The CRMS shall cater to all complaints that are received through the following communication channels:

1) PhilSys help desks
2) PhilSys Fixed Registration Centers
3) PhilSys Mobile Application
4) Official PhilSys website(s) and email address(s)
5) Letters sent via postal services (including handwritten ones)

c. The CRMS also retrieves the list of current incidents detected at the infrastructure level and inform CRMS operators accordingly. This requires an interface between CRMS and EMS. The CRMS also produces and disseminates activity reports on a regular basis.

6.4.3.4 Enterprise Management System

The EMS is intended to enable seamless management of the entire IT Infrastructure, all hardware and software, including network (LAN, WAN) and remote office infrastructure used for PhilSys. The functions of the EMS are as follows:

a. Monitoring of PhilSys IT infrastructures (servers, databases, network) and processes (including backups)
b. Incidents management
c. SLA management including generation of reports
   Generation of SLA-related reports.
d. Automated correlation of events
e. Log incidents

6.4.3.5 Knowledge Management System (KMS)

The KMS is a system that enables identification, capture, evaluation, retrieval and sharing of PhilSys information assets. These assets include documents, policies, procedures and expertise or experiences of PhilSys personnel. The KMS integrates with Business Intelligence and Analytics System, PhilSys Registry, Card Management System, Authentication Management System, IDMS and other PhilSys components.

The following are minimum functions of the KMS:

a. Store new document/material
b. Search or retrieve document/material
c. Share internal documents
d. Display documents

6.4.3.6 Learning Management System (LMS)

The LMS is a system that enables PSA to handle training and knowledge transfer of various PhilSys concepts and processes to PSA users. The LMS will remain an integral part of the portal where the registered users opt for different training programs and undergo training online using audio/video, online presentations, FAQs, Quiz, functional flow documents. The Training records as well as training requirements for users would be maintained by the LMS.

The following are minimum functions of the LMS:

a. Capture training needs of different types of users for analysis

b. Monitor trainings completed by different users and send reminders to users

c. Capture feedback of trainings from Trainees

6.4.3.7 Identity and Access Management System (IAMS)

The IAMS is a system that provides PSA the ability to manage and control access to the PhilSys Information Systems of PhilSys operators and users, software and hardware. The IAMS enables PSA to securely store identity and profile data and data access policies to ensure protection of personal information and only information that is necessary and relevant is shared. This system interfaces to all internal and external PhilSys applications.

The following are minimum functions of the IAMS:

a. Manage access control for all PhilSys users

b. User's Log-in/Log-out

c. Log all transactions (including granular changes brought to access rights).

6.4.3.8 Central Workflow Engine

Central Workflow Engine is the central workflow / orchestration engine of the PhilSys Registry. It manages PhilSys identity records, registration applications, and processing throughout the identity lifecycle. It interfaces with all internal (e.g. IDMS, PSNGTMS, ABAS, SMS, Gateway, etc.) and external applications (e.g. Card Production services).

The following are the minimum functions of the CWE:

a. Forward card personalization packets to CPMS

b. Forward transaction packets between PhilSys components

c. Check if submitted credentials include biometrics

d. Forward 1:1 biometric authentication request to ABAS

e. Start, stop, and monitor the status of workflows

f. Track resource utilization of the runtime engines

6.4.3.9 Support Systems

In support of PhilSys operations and management, the following support systems will be required to provide general analytics, access management to systems and services for authorized personnel, and for the management of help desk queries.

6.4.3.9.1 Access Management

Access to PhilSys Information System should be restricted to authorized personnel either in the operational context (e.g. PhilSys Registry systems) or for operators accessing the Registration software in a PhilSys Fixed Registration Center. System administrators should sign-in to applications with strong authentication (e.g. 2-factor authentication).

6.4.3.9.2 Technical Help Desk / Incident Management System

Support issues and contact with users and clients must be recorded, tracked and resolved in an incident management system. This system must support, but is not limited to, the following functionality:

a. **Contact Management / CRMS** – ability to manage contacts with users from multiple channels (e.g. email, phone, web portal) and to consolidate a history of interactions with the help desk or operational staff responding to issues.

b. **Technical Help Desk** – managing of queries from PhilSys internal users including staff of PhilSys Fixed/Mobile Registration Centers, accredited trusted service providers and Relying Parties.

c. **Ticketing Management and Workflow** – the recording and organization of incidents and user contact points into tickets and the ability to prioritize, track, and manage their resolution efficiently.

d. **Knowledge Base** – compilation of user questions, FAQs, how-to articles, to assist in the support and resolution of recurring and future issues as well as providing self-service facility to users.

e. **Escalation** – capability to route specific issues to specific expert staff or managers in order to resolve pressing issues or reduce the effect of bottlenecks.

f. **Dashboards and Reporting** – to provide real-time views of issue management task (e.g. call center handling), and to prepare management reporting.

g. **Analytics** – the ability to analyze incident management activities and trends, underlying issues and opportunities for change to be identified.

6.4.3.9.3 Information Security

Information Security as a function is the responsibility of all PhilSys personnel. Each system component of Information Security should be developed, and implemented, to observe Security Design Principles as described in *Section 9.7 Information Security*.

6.4.3.9.4 Record History

A record history will be maintained for each application and PhilSys record. This will include events throughout the identity lifecycle such as authentication, data updates, and issuance and delivery of PhilID Cards and PSN tokens.

6.4.3.9.5 PhilID Card Personalization

PhilID Card Personalization covers printing of PCN, demographic information, front facing photograph and QR Code (with embedded metadata).

6.4.3.9.5.1 Personalize PhilID

For registration records that have been successfully de-duplicated, the procedure for personalization of PhilID cards is as follows:

a. The IDMS tags PhilSys Registry records for card printing

b. The CPMS sends requests for batches of records for card printing.

c. The CBU retrieves records for card printing from the PhilSys Registry.

d. CBU performs the following:

  1) Create print files containing PCN, demographic information, front facing photograph and QR Code (with embedded metadata).

  2) Group print files into batches of card production request packets;

  3) Encrypt card production request packets;

  4) Forward production request packets to the CPMS;

e. CPMS receives the batches of records for printing and queues these to CPS for personalization. The CPS is external to the PhilSys Registry and is managed by PSA / BSP.

6.4.3.9.5.2 Send Personalization Status

The CPMS receives the batches of card production request packets and queues these into the personalization process. The CPMS decrypts the card production request packets and uses this information for PhilID card personalization. After the cards are personalized, the CPMS sends information back to the IDMS with the status, the PhilID number, and the serial number of the card (as input to the Card Management System under IDMS). The personal information used for card personalization are automatically deleted after successful personalization of PhilID.

6.4.3.9.6 Card Shipment

The CPMS prepares for the packaging or kitting of the PhilID and other communication materials into individual envelopes. These envelopes are forwarded PFRCs through third party couriers. The Card Shipment status of the envelopes are updated through the CPMS.

6.4.3.9.6.1 Delivery Status

Once the batches of envelopes reach the PFRC, the Delivery Status of the envelopes are updated through the CMS by receiving PFRC Registration Officer/Staff. The updated Delivery Status is automatically replicated in the CPMS.

6.4.3.9.6.2 Card Release Status

When the Registered Person comes to the PFRC to claim his/her PhilID, the PFRC Registration Officer/Staff releases the envelope and PhilID after a successful authentication. The Card Release Status of the associated PSN is updated through the CMS.

6.4.3.9.7 SMS Gateway

A Short Message Service (SMS) Gateway is a website that allows users to send SMS messages from a web browser to people within the cell served by that gateway. It will send a message or a confirmation on every transaction that requires an OTP feature verification.

6.4.3.9.7.1 Send SMS

The Notification System (NS) will handle the sending of SMS messages to Registered Persons ("Send SMS to PSN holders") through the SMS Gateway. The SMS messages will be sent to the registered phone number of the PSN holders for transactions that need verification through a 6 -digit OTP code to complete the login process.

6.4.3.9.8 Admin Portal

Admin Portal allows the PhilSys administrator to manage all aspects of the PhilSys Web Portal. The administrator has proper privileges to monitor and update the portal. The following are the functions within the Admin Portal:

a. **User and Role Account Management**: The administrator can add, delete, update and search users using the Admin Portal. This module is also responsible for editing roles and access of each user. A role will be used to grant different permission levels to different pages or portal instances. A user can have several roles.

b. **Content Management**: This function may provide the repository for portal components including shells, themes, menus, books, pages, layouts, look & feels, portlet categories and portlet producers.

c. **Dashboard PhilSys Operations**: Using this digital dashboard, administrators can track the flows inherent within the business processes of PhilSys. It can be displayed graphically to see the high-level processes and then drill down into low level data.

6.4.3.10 Trusted Service Provider Authentication System (TSPAS)

The SI MUST design, customize and develop Trusted Service Provider Authentication System (TSPAS). This is a middleware system that will be deployed at TSPs and Registered Partners for the authentication services provided by the PhilSys. The TSPAS will have a secure connection to the PhilSys Registry. The devices used by the TSP to connect to the PhilSys are registered and managed by a PSA Admin User using PDMS.

The SI MUST develop this middleware as well as create and document the corresponding API, for TSPs to develop their own client applications.

6.4.3.10.1.1 Create Auth / eKYC Request

The SI MUST develop an App for creating Authentication / eKYC Request. This App is used when an eKYC authentication request from a Registered Person is coursed through a TSP / RP. The AMS will receive the authentication requests, process them and send back the authentication result to the requesting registered TSP / RP.

6.4.3.10.1.2 Read Auth / eKYC Response

The SI shall develop an App designed for reading eKYC Authentication transactions coming from the registered TSP / RP. When an Authentication / eKYC transaction is received, the AMS uses this App to read the authentication transaction. When the transaction is verified as a valid request, the AMS will send a response through a form of notification by SMS or to a valid Email.

6.4.3.10.1.3 Check Auth Request

When a Relying Party forwards an authentication request to PhilSys through a public-facing API Management System (APIMS), the APIMS checks whether the Relying Party has the correct system credentials and if the RP is indeed authorized to access the APIs.

6.4.3.10.1.4 Forward Auth Request

When the TSP receives an authentication request, the TSP software forwards the request to the AMS.

6.4.3.10.1.5 Forward Auth Response

When the TSP receives an authentication response from AMS, the TSP software forwards the response to the Relying Party.