7 Technical Solution Requirements – PhilSys Information System

7.1 Overall Technical Design

The following diagram illustrates the overall logical design of the PhilSys Registry.

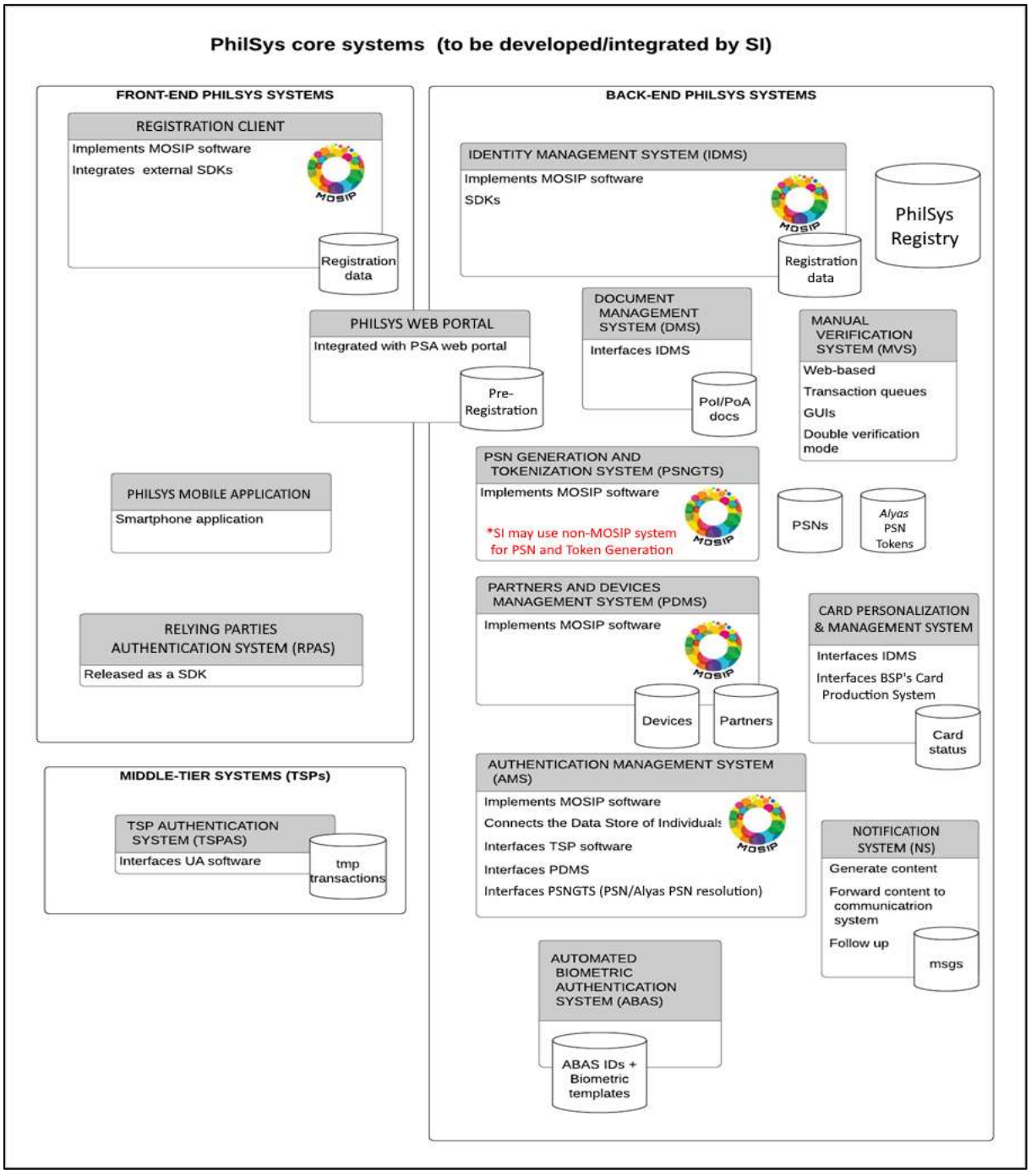

Figure 13. PhilSys Logical Design

*Please note that neither the PhilSys support systems nor data stores are represented in the above diagram.

7.2 Solution Design Requirements

The PhilSys Registry is composed of various software components that operate in unison to deliver the needed information within the defined processes outlined in this section. The PSA has recognized the complexity of organizing and managing various information systems in the context of PhilSys requirements. The design principles of the PhilSys Registry requirements are outlined below.

7.2.1 Service-Oriented Architecture

Commercial off-the-shelf (COTS) and configured software components (i.e. Open Source Software) must be compliant to Service Oriented Architecture (SOA), particularly employing microservices development and development approach. This enables any of the software components to be loosely coupled with each other, reducing the risk of technology lock-in. This approach provides the flexibility for PSA to implement better software components without entirely redeveloping and redeploying unaffected systems or modules.

7.2.2 Container Architecture

For development and deployment, the container-based architecture is proposed for seamless application development and deployment. Components should be developed as micro services.

SI should use a Container Architecture tool for the entire development life cycle.

Following principles need to be followed to develop a container architecture:

a. Use containers for application and data packaging and deployment
b. During system design, Container Orchestration layer needs to be considered. Container-based architecture has a rich API based architecture and support micro services.
c. Should support open source and open standards like OCI, CNCF, Java, other frameworks like Node.JS, NoSQL, etc.

7.2.3 Micro Services

Custom built systems and applications must follow the micro services design for the PhilSys Information System. Any custom-built systems and applications must undergo full technical vetting and approval of the PSA, before any development takes place. Following a micro service design allows the

full modularity of services at the level of the transaction. This modularity also provides PSA the flexibility it needs to manage these services more efficiently.

7.2.4 API-driven Data Communications

a. Software components must be capable of connecting through an Application Programming Interface (API). Using the API approach to data communications enables PSA to fully abstract the data stores apart from the application layer. This level of abstraction provides PSA an increased degree of data access control visibility on what data is being accessed by which system or application. PhilSys APIs should be designed using open standards. SI must ensure that APIs are:

   1) Scalable: To maintain service levels when demand increases or when dealing with unexpected events and adhere to security policies and guidelines defined by the PSA

   2) Reusable where possible so the PSA does not duplicate work

b. In addition, APIs should:

   1) Follow the industry standard and where appropriate build APIs that are RESTful, which use HTTP verb requests to manipulate data.

   2) Return data as URIs for certain data. Where appropriate, use specifications that use hypermedia, including CURIES, JSON-LD or HAL.

   3) Use JSON to represent API responses (unless there are clear advantages to use another established standard e.g. SAML)

   4) Use the Unicode Transformation Format (UTF-8) standard when encoding text or other textual representations of data.

   5) Be configured to respond to 'requests' for data rather than 'sending' or 'pushing' data.

   6) Maintain logs for requests particularly where personal data is requested or affected.

   7) Be clearly documented. Use the Open API 3 Specification where appropriate for generating documentation and include samples where possible.

7.2.5 Conformance to PeGIF Standards, Data Privacy and with Global Standards

Software components MUST conform to the prevailing PeGIF[7] Standards and Data Privacy Technical Issuances of the National Privacy Commission. Furthermore, software solutions must align with the

[7] Philippine eGovernment Interoperability Framework (PeGIF), http://i.gov.ph/pegif/

Catalog of Technical Standards for Digital Identity Systems[8]. In the event that the current PeGIF and Data Privacy Standards were found insufficient, the System Integrator may recommend to PSA to include emerging standards for use in PhilSys Implementation.

7.2.6 Secure login to all PhilSys applications

The SI MUST design, develop/customize, install and maintain a comprehensive technical solution for all PhilSys users to securely log into all PhilSys applications. The proposed solution MUST allow for a high level of security (multi-factor authentication), accountability (non-repudiation, centralized tamper-proof activity logs). It MUST be fully integrated with the IAMS (for more details, please refer to section 7.4.10). It should also cater to the need for offline login of registration operators. The solution MUST be described in great detail by the bidder in its technical proposal and will be considered in the frame of the technical evaluation of the bids.

7.2.7 Data Exchange with Third Parties

a. The SI should implement APIs for exchange of data with Third Parties in adherence with PSA's policies.

b. Clear audit trails should be maintained regarding data exchanged with third parties and how the data is used.

c. Data exchange through direct network connections and sharing of unencrypted data should be strictly avoided.

d. SI should implement procedures to ensure that the non – repudiation of data can be clearly established.

7.2.8 Integration Channels

a. PhilSys Information System will need to integrate with external systems such as RPs and TSPs. Within the PhilSys Software System, there will also be a need to integrate different components.

b. There are three major channels of integrations namely Open API's, ETLs and SFTP. Open API's would be the major integration channel for integration with external and internal applications. These API's would be exposed to external systems (TSP/RP), biometric devices, web applications, mobile Applications and portals using API Gateways.

[8] http://documents.worldbank.org/curated/en/707151536126464867/pdf/129743-WP-PUBLIC-ID4D-Catalog-of-Technical-Standards.pdf

c. For internal consumption of services within PhilSys-DS applications, these API's shall also be exposed using an internal Enterprise Service Bus (ESB) and/or an API Gateway.

d. Advantages of using API based integration are provided below:

1) **Choice / Flexibility**: Users across the PhilSys ecosystem gets the choice and flexibility of using their preferred application and user interface without having to depend on a single portal.

2) **Innovation**: Application ecosystem can innovate in terms of providing all kinds of features such as offline capabilities, alerting capabilities, mobile / tablet interfaces, and so on as device and user interface technologies evolve without PhilSys Information System needing to build all possible features into a single portal.

3) **Agility**: When entire system is loosely coupled via components exposing APIs, it allows individual API implementations to change without having to affect the rest of the system. Building the entire system as a monolithic application completely takes away the agility of PhilSys to adapt to evolving policy decisions and rules. API driven approach allows encapsulation of components and data models without every other part of the system knowing the details. API based design also allows automated testing of the entire system to ensure changes are quickly tested in a completely automated way to avoid regression.

4) **Manageability**: API based systems allow easy manageability in terms of monitoring, auditing, and performance analysis. In addition, individual APIs can be version controlled and deployed / upgraded / rolled-back instead of entire application being released, tested, and deployed.

5) **Scale**: For a national system like PhilSys to scale, load has to be distributed across various systems. This is key for responsive user experience as well as core system scaling. Instead of entire application being monolithic and access via web portal, if should be built with stateless APIs that can be scaled horizontally. Most critically, user interface load is distributed to external applications making PhilSys Information System truly a lean platform that can be scaled to country's need. Providing stateless APIs allow load balancing across Data Centers for scale and distributing user interface load to third party applications.

6) **Data consistency**: Providing APIs to access all data models and functionality ensures data is not duplicated unnecessarily. This offers a single source of truth of data to be managed via common APIs. In addition, providing centralized data validation, digital signature, etc. ensures data is consistent and accurate across the system.

7) **Security**: Data security is paramount to PhilSys Information System. Accessing data only via APIs ensure centralized management of security controls. Encapsulating access control, auditing, confidentiality (via encryption), and integrity (via signatures) is only possible via common APIs.

8) **Cost-effective**: Most importantly, PhilSys Information System can be kept simple, scalable, API driven, 3rd party application driven, and agile to meet the changing needs

of residents, ecosystem partners, and policy makers, which ensures that the cost of the entire system is kept minimal while providing all core features and functionalities.

9) **ETL** would be used for integration of all application data with the Data Warehouse, Business Intelligence, Analytics, Fraud application, etc.

10) **SFTP** would be used for secured transfer of Registration packets from Registration centers to IDMS.

11) **Enterprise Service Bus / Integration** Middleware: For hosting all the web service/API endpoints for internal consumption and external consumption by Pre-Registration and other applications.

7.3 PhilSys Registry System

The following are components of the PhilSys Information Systems:

Table 41. Components of the PhilSys Information System

Components of the PhilSys Information System	Minimum Functions to be Supported
Front-End PhilSys Core Business Systems	
Registration Software (REGS) For PhilSys Fixed Registration Center and PhilSys Mobile Registration Center	REGS-F01 Fetch Pre-Registration Record REGS-F02 Register Applicant REGS-F03 PSA Operator Login / Logout REGS-F04 Update demographic data (including mobile phone number and email address) REGS-F05 Update biometric data
PhilSys Fixed Registration Center – Authentication Using ABAS	ABAS-F01 Authenticate a registered person; Match (Fingerprint/Iris/Face)
PhilSys Fixed Registration Center – Other Services (FSVC)	FSVC-01 Get application status FSVC-02 Record grievance / retrieve status FSVC-03 Request new PhilID FSVC-04 PhilID Card collection (through CPMS) FSVC-05 Integrate with Payment Gateway FSVC-06 View Transaction History FSVC-07 Report of Lost PSN / PSN Retrieval FSVC-08 Perform Lock-in / Lock-out PSN As well as all functions available on the Web Portal (e.g. generate PSN token, lock authentication, etc.
PhilSys Fixed Registration Center – Queueing System (QUES)	QUES-F01 Generate Queue Numbers QUES-F02 Display Queue Numbers currently being served
PhilSys Web Portal (PWP)	PWP-F01 Request Card Replacement/ Check Status PWP-F02 Check Registration Status

Components of the PhilSys Information System	Minimum Functions to be Supported
	PSNG-F01 Display Active Alyas PSN PSNG-F02 Generate Alyas PSN PWP-F05 Enable Pre-Registration and Appointment PWP-F06 Lock/Unlock PSN PWP-F07 Report of Lost PSN PWP-F08 Request New PhilID PWP-F09 Submission of Grievance Reports PWP-F10 User's Login /Logout PWP-F11 View Card Replacement Status PWP-F12 View Transaction History PWP-F13 View FAQs (Locate PhilSys Fixed Registration Centers and other information) PWP-F14 Lock PSN Authentication PWP-F15 Update Demographic Data (address only) PWP-F16 Generate and Display QR code for Alyas PSN token PWP-F17 Generate and Display a digitally signed QR code for Alyas PSN token
PhilSys Mobile Application (PMA)	PMA-F01 User's Log-in/Log-out PMA-F02 Authenticate using PSN and OTP via SMS PMA-F03 Display all active Alyas PSNs PMA-F04 Generate Alyas PSN PMA-F05 Generate and display QR code for a given Alyas PSN PMA-F06 Generate and display full picture of PhilID Card for a given Alyas PSN PMA-F07 Report of Lost PSN PMA-F01 Check / Request Card Replacement Status PMA-F08 Request New PhilID PMA-F09 Submission of Grievance Reports

Components of the PhilSys Information System	Minimum Functions to be Supported
	PMA-F11 View Card Replacement Status PMA-F12 View Transaction History PMA-F13 View FAQs (Locate PhilSys Fixed Registration Centers and other information) PMA-F14 Lock PSN Authentication PMA-F15 Update Demographic Data (address only) PMA -F16 Generate a digitally signed QR code
Pre-Registration Module (PREG)	PREG-F01 Book an appointment for registration PREG-F02 Enter demographic data & upload supporting documents PREG-F03 Appointment notification, rescheduling and cancellation PREG-F04 Send resident data to registration center before appointment, which can be used during registration
Back-end PhilSys Business Systems	
Identity Management System (IDMS)	IDMS is the registration processor core of MOSIP application suite IDMS-F01 Lock/Unlock PSN IDMS-F02 New ID Issuance IDMS-F03 Update Individual's Information IDMS-F04 De-activate Individual's ID IDMS-F05 Re-activate Individual's ID IDMS-F06 Biometrics Quality Check IDMS-F07 Deduplication – Demographic, Biometrics IDMS-F08 ABIS Integration (Incl. ABIS Middleware) IDMS-F09 PSN Assignment IDMS-F10 Store/Update ID Repository IDMS-F11 Capture Audit Trails/Analytics Data

Components of the PhilSys Information System	Minimum Functions to be Supported
Central Workflow Engine (CWE)	The CWE can be seen as the central workflow / orchestration engine of the PhilSys Registry CWE-F01 Forward card personalization packets to CPMS CWE-F02 Forward transaction packets between PhilSys components CWE-F03 Check if submitted credentials include biometrics CWE-F04 Forward 1:1 biometric authentication request to ABAS CWE-F05 Start, stop, and monitor the status of workflows CWE-F06 Track resource utilization of the runtime engines
Document Management System (DMS) / Document Retrieval	DMS-F01 Manage access to uploaded supporting registration documents DMS-F02 Store registration forms and supporting documents DMS-F03 Store, search, display and share PhilSys internal documents
Manual Verification System (MVS)	Manually review and resolve exceptions raised by various PhilSys modules (including potential duplicates based on matching scores returned by the ABIS). MVS-F01 User Login and Logout MVS-F02 Fetch Manual Verification Case MVS-F03 Resolve case MVS-F04 Escalate case
PSN Generation and Tokenization Management System (PSNGTMS)	PSNG-F01 Generate PSNs

Components of the PhilSys Information System	Minimum Functions to be Supported
	PSNG-F02 Generate and managePSN tokens (PCNs, Alyas PSNs, common PSN tokens for interoperability among selected RPs and internal PSN tokens such as the ones to be used by the ABIS)
Card Personalization Management System (CPMS)	Integration with PhilID Card personalization to the external personalization system(s). Keep track of PhilID personalization orders. CPMS-F01 Queue batches of card for personalization CPMS-F02 Transmit card for actual printing. CPMS-F03 Perform quality checks CPMS-F04 Delivery to designated PhilSys Fixed Registration Centers
Card Management System (CMS)	Provide services to Registered persons such as request for card replacement, information on status of card replacement, card releasing and card delivery status CMS-F01 Card replacement request CMS-F02 Information on status of card replacement CMS-F03 Card Releasing CMS-F04 Card delivery status
Partners and Devices Management System (PDMS)	Register or dereference (blacklist) authentication partners and devices. Generate partner codes PDMS-F01 Add, suspend, revoke, edit profile, display activity, edit reports of PFRC's, Relying Parties, TSP's, Registered devices for authentication. PDMS-F02 Manage (generation and distribution) license and keys

Components of the PhilSys Information System	Minimum Functions to be Supported
	RPDM-F03 Retrieve the status of a partner or a registered device
Authentication Management System (AMS)	AMS-F01 Process authentication/eKYC Request AMS-F02 Process authentication/eKYC Response AMS-F03 Log Transactions AMS-F04 OTP Authentication AMS-F05 Check validity of incoming authentication requests. AMS-F06 Dispatch authentication AMS-F07 Carry out demographic matching AMS-F08 Carry out OTP authentication AMS-F09 Forward the request to the Automated Biometric Authentication System (ABAS) in case of a biometric-based authentication. AMS-F10 Receive authentication result(s), consolidate and forward back to the requesting party.
Automated Biometric Authentication System (ABAS)	Process multi-modal biometric-based authentication (1:1 matching). ABAS-F01 Match (Fingerprint/Iris/Face) ABAS-F02 Manage Records (add/update/delete) ABAS-F03 Create Templates from Images
Automated Biometric Information System (ABIS)	ABIS-F01 Integration with ABIS ABIS-F02 Perform 1:N Matching (Fingerprint/Iris) ABIS-F03 Manage Records (add/update/delete) ABIS-F04 Create Templates from Images Note: ABIS functions ABIS-F02, ABIS-F03, and ABIS-F04 are out of scope for SI.
Notification System (NS)	Send notification (SMS / Email) to PSN holders (gateway)

Components of the PhilSys Information System	Minimum Functions to be Supported
	NS-F01 Generate OTP NS-F02 Send OTP via SMS NS-F03 Send OTP via E-mail NS-F04 Send SMS/E-mail
Back-End PhilSys Support Systems	
Fraud Detection and Management System (FDMS)	Real-time and offline detection of potential fraud cases FDMS-01 Capability to lock authentications/eKYC for a given registered person using a rules-based model FDMS-02 Flag transactions forwarded by the MVS for investigation FDMS-03 Provide real-time risk score, and reason code during registration/authentication FDMS-04 Generate alerts after analyzing batch-based data FDMS-05 Extensive and out of the box (OOTB) profiling of data in existing source databases, data warehouses or data marts FDMS-06 Present profiling results in textual report format
Business Intelligence and Analytics System (BIAS)	Provide tools, applications and methodologies, inclusive of OOTB standard analytical templates, dimensions, secure extraction methods, and/or schemas to analyze data from PhilSys sub-systems and external sources (such as Card Production and Delivery, Trusted Service Providers and Relying Parties), develop and run queries against that data and create reports, dashboards and data visualizations to make the analytical results available to PhilSys management and decision-makers. BIAS-F01 Generate data analytics

Components of the PhilSys Information System	Minimum Functions to be Supported
	BIAS-F02 Provides Dashboard (management and operational)
Customer Relation Management System (CRMS)	Collect and manage complaints from members of the public and PSA partners via multiple communication channels, including (but not limited to) PhilSys helpdesk and Fixed Registration Centers Analyze and record incidents CRMS-F01 Retrieve Complaint Status CRMS-F02 View Reports of Lost PSN / PSN Retrieval CRMS-F03 Generate Ticket Number CRMS-F04 Produce Activity Reports
Technical Helpdesk (TDES)	TDES-F01 Generate helpdesk ticket number TDES-F02 Perform remote troubleshooting TDES-F03 Route issues to appropriate unit TDES-F04 Generate Reports
Enterprise Management System (EMS)	Monitor PhilSys IT infrastructures (servers, databases, network) and processes (including backups) EMS-F01 Monitoring of all critical IT infrastructures including software applications, storage systems, servers, networks using SNMP traps or equivalents EMS-F02 Monitoring of backups EMS-F03 Incidents management EMS-F04 SLA management including generation of reports EMS-F05 Automated correlation of events EMS-F06 Log incidents
Knowledge Management System (KMS)	Store, search, display and share PhilSys internal documents

Components of the PhilSys Information System	Minimum Functions to be Supported
	Collaborate (workflow and notifications) KMS-F01 Store new document/material KMS-F02 Search document/material KMS-F03 Share internal documents KMS-F04 Display documents
Learning Management System (LMS)	LMS-F01 Capture training needs of different types of users for analysis LMS-F02 Monitor trainings completed by different users and sending reminders to users LMS-F03 Capture feedback of trainings from Trainees
Identity and Access Management System (IAMS)	Manage access control for all PhilSys internal users such as operators and administrators. IAMS-F01 Manage access control for all PhilSys Internal users IAMS-F02 User's Log-in/Log-out (internal) IAMS-F03 L og all transactions (including granular changes brought to access rights)
Asset / Tracking Management System (ASMS)	Track the lifecycle of PhilSys assets from arrival to disposal (purchase, arrival, provisioning, warranty, AMC, repair / maintenance, renewal dates) Support customized metadata for the asset management system ASMS-F01 Route, track and synchronize instructions between PhilSys components ASMS-F02 Track lifecycle of PhilSys assets ASMS-F03 Track PhilSys hardware and software
API Gateway (APIMS)	Act as a single point entry for group of micro services.

Components of the PhilSys Information System	Minimum Functions to be Supported
	APIMS-F01 Check if Relying Party has correct credentials APIMS-F02 Transform message to API format
Audit Trail (AUDT)	Logging of PhilSys transactions for auditing and traceability purposes. AUDT-F01 Logging of PhilSys Transactions
Back-up / Restore Management (BRMS)	BRMS-F01 Backup BRMS-F02 Scheduling and Management BRMS-F03 Offsite Backup BRMS-F04 Automation Support BRMS-F05 Recovery/Restore
Network Operation Center (NOC)	NOC-F01 Integrate the EMS solution, dashboard with the NOC. NOC-F02 Provide a Video Wall with ability to display SLAs, key metrics and data from the EMS Dashboard. NOC-F03 Fully Secured access to NOC NOC-F04 Provide a unified view of all the DC operations, IT Infrastructure and Services.
Security Operation Center (SOC)	SOC-F01 Management of security incidents, inclusive of incident classification, BIA, and incident closure. SOC-F02 Establish a security exception management process. SOC-F03 Identify and report information security exceptions against PhilSys security policies and processes. SOC-F04 Integration and interoperability to Computer Emergency Response Team (CERT)
Payment and Billing Solution (PBS)	PBS-F01 Create payment transaction records PBS-F02 Record an audit trail of all actions

Components of the PhilSys Information System	Minimum Functions to be Supported
	PBS-F03 Payment refund PBS-F04 Payment status tracking
Admin Portal (ADPO)	ADPO-F01 Set up Platform Data, Process Flows, ID Definition, Configuration, and Security Policy (Through back-end process). ADPO-F02 Manage (Create, Update, View, Activate/Deactivate, Map/Un-map/Re-map/Decommission) the resources. (Through API and UI Screens) ADPO-F03 Map the resources (Users, Machines, and Devices) to a registration center (Through APIs) ADPO-F04 Manage the master data (Create/Update/Activate/Deactivate). (Through APIs) ADPO-F05 Manage approval requests for creation and updating of resources and master data. ADPO-F06 Manage personal account details (Reset Password, Forgot User Name, Change Password, Unlock Account, and Edit Personal Details) ADPO-F07 Activate/deactivate UIN ADPO-F08 View status of packets
Database Activity Monitoring Solution (DAMS)	DAMS-F01 View Transaction History DAMS-F02 Monitor and audit all database activities DAMS-F03 Generate alerts/notifications whenever policy violations are detected
Middle-tier systems that will be deployed at authentication partners (TSPs and RPs)	
TSP Authentication System (TSPAS)	TSPAS-F01 Receive authentication/eKYC requests from the different Relying Parties (RPs) TSPAS-F02 Validate and e ncapsulate authentication/eKYC request.

Components of the PhilSys Information System	Minimum Functions to be Supported
	TSPAS-F03 Forward encapsulated authentication/eKYC request to the PhilSys Authentication Management System (AMS) TSPAS-F04 Process responses sent back by PhilSys back-end system and forward to the requesting RP
Pilot systems (required for pilot use cases at two RPs only (PSA and DSWD): this software application will **not** be massively deployed)	
RP Authentication System (RPAS) – sample application	RPAS-F01 Create authentication request RPAS-F02 Send API request to generate OTP over SMS RPAS-F03 Send authentication/eKYC request to TSP RPAS-F04 Process authentication/eKYC response received from TSP (display transaction result) RPAS-F05 Check credentials provided in API request

Please note that in some cases, a "system" can consist of more than one software application.

7.4 PhilSys Registry Software Capabilities

The SI shall be responsible for implementation and maintenance of the PhilSys Information System's software applications. In order to implement the PhilSys Information System, the SI shall use or configure MOSIP to develop the core components of PhilSys, develop other components using OTS/COTS products and integrate all PhilSys applications.

It shall be the responsibility of the SI to provide a fully integrated software suite that includes the following minimum capabilities:

Table 42. Minimum Required Capabilities of PhilSys Software System

Key Components	MOSIP	BioSP	SI (Develop / COTS / OTS)
Registration Software	✓		
Identity Management System	✓		
PSN Generation and Tokenization System	✓		✓ (SI may use non-MOSIP PSN generation and tokenization System)
Authentication Solution	✓		
ABAS			✓ (integrating the SDKs provided by the BioSP)
Integration Middleware			✓
Pre-Registration App	✓		✓
Central Workflow Engine			✓
ABIS		✓	
Manual Adjudication System		✓	
Manual Verification System			✓
Fraud Management			✓
PhilSys Web Portal			✓
PhilSys Mobile Application			✓
Business Intelligence and Analytics			✓
Partners and Devices Management System			✓
CRMS			✓
DMS			✓
Identity and Access Management			✓
Knowledge Management			✓

Key Components	MOSIP	BioSP	SI (Develop / COTS / OTS)
TSP software			✓
RPAS sample application			✓
EMS			✓
Card Personalization Management System			✓
Card Management System			✓
Queueing System			✓

Provision of the application development and testing environment along with all the necessary tools, artefacts, sub-systems required for development, testing and maintenance of the PhilSys Information System would be the responsibility of the SI. In case the SI has not considered any component / service which is necessary for implementation of the PhilSys Information System, the same shall be brought by the SI at no additional cost to the PSA.

7.4.1 MOSIP Application

The MOSIP application suite comprises of the following applications (detailed functionalities of these applications can be been seen in **https:/docs.mosip.io**). A brief snapshot of the overview of the MOSIP is given below.

7.4.1.1 Pre-Registration Module

This application shall allow the residents to submit pre-Registration information through a web-based portal and obtain an appointment at the designated PhilSys Fixed Registration Centers.

The SI MUST design, develop, install and maintain the pre-registration application.

The SI MUST develop and publish an API and a secure web service (to authorized users only) to support the “pre-registration via a pre-enrolment agent” use case described in Section 6.

7.4.1.2 Registration Software

This application shall be hosted on the Registration Kit equipment of the Registration Officer and will be used for registration of the Applicant. The Registration Officers would login using their own PSN and biometrics or USB FIDO dongle. The Registration Client must recognize legitimate PSA users

before any access to the internal features are permitted. The user credentials must be pre-loaded centrally before the Front-end are deployed to field operations. The Registration Client must be capable of user-opted logout and automated logout due to system time out.

Through this software, the Registration Office will fetch the pre-Registration information (wherever applicable), enter remaining demographic information, scan supporting documents, capture photograph and biometrics (both iris, face and fingerprints). Resident information once captured would be stored in the Registration Kit equipment in an encrypted format for onward transmission to PhilSys Registry in a secure format.

7.4.1.3 Identity Management System (IDMS)

a. This application shall receive the Registration packet and process it in a sequential staged manner from the validation of the packet to the generation of PSN number and intimation of the PSN to the Registered Person. 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 for the registration process.

b. The key functionalities of the application are provided below:

   1) **Secure Synchronization –** This IDMS would have capability to send response back to the registration software upon successful receipt of the packet in a secure fashion from the client.

   2) **Registration Packet Verification** – This function will perform antivirus checks to ensure packet is not corrupted during transmission.

   3) **PKI Decryption –** private keys managed by an HSM device will do PKI decryption.

   4) **Transaction Management** – The complete transaction lifecycle of a packet from decryption to the ID generation is broken down into various stages having relevant checkpoints assigned to each stage maintained in both memory and persistent database. This enables transaction processing restart at the point of failure rather than a rollback to the 1st stage.

   5) **Structural Validation and Standardization** – The module is responsible for performing structural change checks of the packets including tampering and corruption. This includes migration of data from packet into multiple standardized data stores for subsequent processing.

6) **Quality Check** – The quality check will be performed on the registration packets. This will check whether the registration officer is authorized and active, registration center is active, etc.

7) **Demographic De-Duplication –** Data fed to the data stores from the packet is then processed in a de-duplication engine with rules checking for duplication of demographic details of the packet with other successfully processed packets stored in DS.

8) **Interface with ABIS for Biometric De-duplication** – Post demographic de-duplication activity, biometric information is shared with ABIS management layer through this interface.

9) **PSN Generation** – IDMS will access the PSN Generator currently deployed for allocating PSN. Thus, every successful transaction confirmed from all stages will be assigned a PSN number from the PSN Generator.

10) **Event Generation** – All the participating modules of transaction processing will generate events based on the defined business rules. These alerts will be fed in a data store and will be accessed by the Business Intelligence module to generate insights supporting decision making on operational effectiveness.

11) **Sequential Event Driven Flow –** The transaction processing will be done through well-defined stages running in sequence as well as in parallel based on the complexity assigned to the transaction.

12) **ID Dispatch** – This module will have the feature to dispatch the successfully generated PSN to the respective resident through email/SMS.

13) **Registration Reporting** – MIS module will generate reports detailing the operations conducted at each registration center against the defined KPIs of registration center admin and registration center officer.

14) **Identity Repository –** For the registration packets for which PSN has been allocated, the IDMS would update the identity repository that will contain PSN, Demographic Data, Biometric Templates, etc., which may be used for the purpose of delivery of authentication and eKYC services. The application will also have the feature to update identity repository whenever an update request is received for changes in demographic/biometric data.

7.4.1.4 PSN Generation and Tokenization Management System (PSNTGMS)

The SI MUST design, develop, test, install and maintain the PSN Generation and Tokenization Management System (PSNTGMS) that will allow PSA operators to review cases declared as exceptions by the various components of the PhilSys.

The PSNGTMS MUST support all functions described in Section 6. In particular, it MUST enable the functional requirements shared in Section 6.2.2, related to the model of enabling data sharing among selected RPs outside the scope of the PhilSys. Each correlation space MUST have a unique identifier,

and the PSNGTMS MUST be interfaced with the PDMS to retrieve information related to the onboarded RPs.

7.4.1.4.1 Requirements related to PhilSys Card Number (PCN)

a. The MOSIP Number generator process would be used to generate a unique identification number (permanent PSN) for the residents who have successfully been de-duplicated.

b. The IDMS, after successful deduplication of data will access the Number Generator to get a Permanent PSN. Thus, every successful transaction confirmed from all stages will be assigned a Permanent PSN from the MOSIP Number Generator.

c. The SI MUST:

1) Test, install and maintain the MOSIP Number generator;
2) Integrate the corresponding MOSIP module to that end; and
3) Develop / configure the MOSIP generator and integrate the all PhilSys applications that need to process PSN / PCN and tokens.
4) This system is called PSN Generator and Tokenization System (PSNGTMS)

7.4.1.4.1.1 PhilSys Card Number (PCN)

a. Each time a new PhilID Card needs to be personalized; the system will generate a PCN that will be embedded in the PhilID card personalization order.

b. A PCN is a PSN token that is associated with a PhilID card. It expires whenever the corresponding PhilID card is declared lost or a new PhilID card is requested for.

c. The PSNGTMS MUST feature the generation and revocation of PCNs.

7.4.1.4.2 Requirements related to Alyas PSN

a. An *Alyas* PSN is a PSN token used in the frame of an authentication / eKYC transaction.

b. An *Alyas* PSN MUST be linked to a set of personal data

c. The PSNGTMS MUST attach and manage a validity period for each *Alyas* PSN generated.

d. The PSNGTMS MUST publish an internal service (via open API) allowing another PhilSys System to check: (1) the validity and (2) the restrictions in terms of personal data sharing of a given *Alyas* PSN at any point in time.

7.4.1.4.3 PSNGTMS Requirements Related to Back-end PSN tokens

a. A back-end PSN token is a PSN token used in lieu of a PSN when seeding personal identifiers with some PhilSys subsystems or external systems

b. The PSNGTMS MUST allow for the batch generation, seeding, replacement and revocation of back-end PSN tokens through web-based GUIs.

c. A back-end PSN token does not have to be of the same format than a permanent PSN. The PSNGTMS MUST allow to configure different formats for back-end PSN tokens.

7.4.1.4.4 PSNGTMS Requirements Related to Privacy-preserving Interoperability Services

a. The SI must include technical services to support the Privacy-preserving interoperability services described in 6.2.2.1. The following requirements may vary depending on the proposed solution of the SI.

b. The PSNGTMS MUST allow for the batch generation of PSN token correlation spaces and their assignment to particular RPs.

c. The PSNGTMS MUST allow the management of RPs assigned to specific correlation spaces, including adding and removing RPs as necessary.

d. The PSNGTMS MUST allow the rotation of shared tokens or a particular correlation space.

e. The PSNGTMS MUST support any additional functionality defined by the SI as part of the SI proposed solution for Privacy-preserving interoperability

7.4.1.5 Authentication Solution

The Authentication Solution application shall provide online authentication and eKYC services. The core functions of authentication solution shall include the following:

a. An extractor, from the multimodal SDKs, to be provided by the BioSP, which extracts the biometric templates for Registered Persons and stores the templates in the ABAS database. The ABAS database would be used for biometric based authentication.

b. The biometric matcher, from the multimodal SDKs to be provided by the BioSP, shall compare by **1:1** matching the biometric templates received as part of a biometric authentication request with the biometric template in the ABAS database.

c. A set of open APIs' for different types of authentication (Demographic, Biometric, OTP and eKYC).

d. A cached OTP retained and deemed valid for designated time period. Authentication requests would come to this application through an array of Trusted Service Providers (TSP) and Relying Parties (RP).

7.4.1.5.1 Authentication Management System (AMS)

a. Some Relying Parties will require online authentication of individuals to be confirmed by comparison with the PhilSys Registry. Some services availed by RPs may also require eKYC data to be provided by the PhilSys Registry. This data will be limited to that collected during registration, the scope of personal data that can be shared (as per the registered person's preferences) if an *Alyas* PSN is used (user controlled eKYC) and always within the limitations of the law.

b. Relying Parties will be responsible for obtaining consent from individuals before requesting data as well as ensuring that individuals are informed of the purpose for which this data is required.

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

d. The SI MUST integrate the corresponding MOSIP module to that end.

e. The SI MUST integrate the AMS with all internal and external systems.

f. In particular, the AMS MUST systematically check whether the online authentication/eKYC request emanates from an onboarded RP that can have access to a stable PSN (vertical PSN seeding) or contains a "correlation context" (horizontal PSN seeding). If so, be it and upon successful authentication, the AMS MUST query the PSNGTMS to retrieve the corresponding PSN token (as described in Section 6.2.2). If such a PSN shared token exists, the authentication/eKYC response to be sent back by the PhilSys to the requesting RP MUST include the valid, up-to-date token corresponding to the one included in the incoming authentication/eKYC request. The AMS MUST be interfaced with the PSNGTMS towards that end.

g. The AMS MUST publish all authentication services to the TSPs and the IDMS via an open API. Integration will be achieved via an open standards API made available to TSPs that have completed an on-boarding process with PSA. This API will be protected against unauthorized access and all data in transit will be digitally signed and encrypted to ensure data integrity and confidentiality.

h. All access to the API published by the AMS will be done by TSPs via a secure network connection (private network).

i. All data MUST be cryptographically protected in transit to ensure integrity and confidentiality.

j. The AMS MUST feature One-Time Password (OTP) generation and dissemination by SMS as well as publish an "OTP via SMS" service via open API for Relying Parties to initiate the sending of an OTP to the end user's registered mobile phone number.

7.4.1.5.2 Authentication / eKYC Process

For each incoming authentication or eKYC request, the AMS MUST execute the following operations:

7.4.1.5.2.1 Check Validity

a. Decrypt and check packet security,

b. Check data validity,

c. Validate source (authentication partner and device) by interfacing with the PDMS.

7.4.1.5.2.2 Check Authorization

a. Check whether PSN is an *Alyas* PSN or not,

b. If an *Alyas* PSN is used, resolve the *Alyas* PSN into the corresponding permanent PSN.

c. Check its validity by interfacing with the PSNGTMS; if the PSN token has expired, the authentications / eKYC transaction MUST be rejected with a special error code.

d. If the transaction is of type eKYC, check restrictions on the personal data that can be shared; if the eKYC transaction scope includes sharing personal data that has not been authorized by the registered person when generating the *Alyas* PSN, the AMS MUST reject the eKYC request with a special error code.

7.4.1.5.2.3 Proceed with Authentication

a. Based on authentication request type, dispatch request(s) to the concerned authentication subsystem(s) – including the verification of an OTP,

b. Send a notification via SMS to the PSN holder (if mobile number was provided) containing the reference number of the transaction and stakeholder(s) as well as the result of the authentication.

7.4.1.5.2.4 Housekeeping

a. Log all transactions in the centralized repository of PhilSys logs,

b. Erase all temporary data trails at the AMS level.

7.4.1.5.3 Automated Biometric Authentication System (ABAS)

a. The SI MUST develop, test, install and maintain the ABAS.

b. The SI MUST integrate the 1:1 matching SDK(s) provided by the BioSP to that end (for the three biometric modalities: fingerprint, face and iris).

c. The ABAS MUST support all functions described in *Section 5.4 (Exclusions*

d. *The* following items are out of scope for the SI:

- Mobile Registration Kits including OS and COTS
- ABIS software and hardware for deduplication, Manual Adjudication System and biometric SDKs
- PhilID cards personalization systems (card printers, QA workstations, etc.), services and consumables (pre-personalized blank cards, inks, overlays, etc.)
- PhilID cards delivery/shipping
- Provision of network links (e.g. WAN, Internet connections)
- Software to be deployed at Relying Parties (except for the pilot application to be deployed at PSA and DSWD)
- PhilSys systems' operators and administrators
- SLA monitoring (service)
- Site preparation for PFRCs (location, contracts, payments, and fit out)
- Central sites (Primary DC, secondary DC, DR) and utilities. The PSA shall provide the physical space for hosting IT Infrastructure in a Primary Data Center and Disaster Recovery site as well as Secondary DC.
- Telecommunication costs (SMS)
- Management of Partner Contracting (registration) - for onboarding of TSPs and RPs
- Authentication device management (registration) - conformance procedures
- Payment service provider fees (a payment Gateway is to be jointly identified by PSA/PhilSys and DOF)
- ISO/IEC 27000 series certifications from an accredited body

e. Functional Requirements*)* and *Section 7 (Technical Solution Requirements – PhilSys Information System)* notably, the ABAS MUST feature fingerprint-based and iris-based 1:1 matching.

f. The ABAS MUST run exclusively on commercial hardware.

7.4.1.6 Partner and Device Management System

The Partner and Device management application would cater to the needs of the partner community, which includes the Trusted Service Providers, Relying Parties and Registration officers.

7.4.1.6.1 Partner and Devices Management System (PDMS)

a. The SI MUST test, install and maintain the PDMS.

b. The SI MUST integrate the corresponding MOSIP module to that end.

c. The PDMS MUST support all functions listed in Section 6.

d. The PDMS MUST allow a PSA supervisor to manage (i.e. add, suspend, revoke, edit profile, display activity, edit reports) the following assets throughout their lifecycle:

   1) PhilSys Fixed Registration Centers,

   2) PSA Registration partners,

   3) PSA authentication partners including TSPs, RPs, and Registration operators.

   4) Registered devices for authentication.

   5) The PDMS MUST automatically manage (generation and distribution) license and keys. The SI MUST interface the PDMS with all relevant PhilSys Information System, including security systems such as PKIs in order to do so.

   6) The PDMS MUST allow another PhilSys Information System to retrieve the status of a partner or a registered device at any point in time via an open API.

7.4.1.7 Administration and User Management of Registration Community

The application would allow Administrators to setup new users as Registration officers by allotting them a PSN Number. This application would also allow the setup of PhilSys Service Centers and manage the lifecycle of these centers.

7.4.1.8 View Statistics and KPI's for Registration Community

This application would provide the capability to view statistics related to Registration at various PhilSys Fixed Registration Centers and Mobile Registration Centers such as time taken for Registration, number of Registration packets that failed from a center / Registration officer, etc.

7.4.1.9 Administration and User Management of TSPs and RPs

The application would allow administrators to setup new users as TSPs / RPs along with their credentials etc. This would allow for registration of devices and services permitted (with respect to limited eKYC).

7.4.1.10 View Statistics and KPI's for Authentication Statistics

This application would provide the capability to view statistics related to authentication Partners, such as number of authentications handled by particular TSPs or requests from particular RPs.

7.4.1.11 Drill into Individual Issues

This application would have capability to provide insights into individual performance issues of TSPss, RPs, or Registration Officers to improve their performance.

7.4.2 Manual Verification System (MVS)

a. The SI MUST develop, test, install and maintain the Manual Verification System (MVS) that will allow PSA operators to review cases declared as exceptions by the various components of the PhilSys.

b. This MVS MUST be integrated and handle all sorts of exceptions raised by the IDMS and the FDMS and requiring human verification (consolidated GUIs and controls).

c. The SI MUST develop an integrated module including all tools, controls and GUIs for this Manual Verification System.

d. The MVS MUST allow to process cases declared as exceptions by:

   1) The IDMS before any deduplication takes place (e.g. missing data, bad format, etc.),

   2) The IDMS after the demographic deduplication and before the biometric one,

   3) The IDMS after the biometric deduplication, the FDMS at any point of time.

e. The Manual Verification System MUST provide GUIs, tools and controls so that a PSA operator can review all pending cases

f. The following information MUST be displayed:

   1) Result from the demographic deduplication,

   2) Result from the biometric deduplication (matching score for each biometric modality used by the deduplication as well as multi-biometric, consolidated matching score),

   3) Similarity score for each demographic field,

   4) Portrait photo.

   For security reasons, the cases must be sequentially queued (first in first out), no search function should be available, and demographic data should not be displayed.

g. The MVS MUST allow authorized PSA operators to:

1) Securely login and logout from the application,
2) Review a case,
3) Forward to the IDMS (including litigious cases sent back by the ABIS after the biometric deduplication (potential duplicates),
4) Forward to the fraud detection module.

h. Other technical requirements:
1) The MVS MUST implement queues (one queue per type of manual verification).
2) The MVS MUST be integrated with PhilSys user directory (LDAP / Active Directory or similar).
3) The Manual Verification System MUST allow a PSA Officer to take a final decision in a single click.
4) The MVS MUST be configurable in such a way that a second human operator can review the same case (blind, 2-step verification including a dedicated queue for cases for which the decision of the first and second reviewers differ). This second-step verification can either be requested by the first reviewer or enforced by an administrator for all cases for one or more job queues.
5) The MVS MUST offer the possibility to cancel the final decision for a limited, configurable time (in case an operator clicks on the wrong button).

i. All transactions happening at the MVS level MUST be logged (type of transaction, user ID, timestamp). Logs MUST be digitally signed using a hash to prevent tampering and included in backup policy / scope.

7.4.3 Central Workflow Engine (CWE)

a. The PhilSys uses a microservices architecture and the application suite is composed of large number of microservices. There are multiple use cases spanning the whole ecosystem. Each use case may involve interaction with one or more microservices as required. From a computing and end user perspective one can classify the uses cases broadly into the following:

1) Interactive with real time responses (there is an interaction with the user - via browser or mobile application)
2) Interactive with delayed responses/ notifications (there is notification to the user via a mobile app/sms/e-mail notification)
3) Non-Interactive – long running use-cases which may or may not involve any human interaction

b. The SI MUST use a rule-based, configurable workflow engine which will orchestrate jobs across one or more microservices for real time responses.

c. For use cases which do not need real time responses the SI can Customize COTS/Open Source workflow engines which orchestrate requests across multiple microservices/applications which may or may not have human interaction. The proposed workflow engine (based on open standards) should have the following characteristics:

   1) A Graphical User Interface for modelling and creating workflows, the modelling tool should be based on open standards.
   2) A Graphical User Interface for deploying the workflows, there should also be command line options/APIs for automating the deployment process.
   3) A runtime engine which executes these workflows – the engine should be horizontally scalable by deploying multiple instances as and when there is increased load.
   4) The engine should be highly available and should not have any single point of failure.
   5) The engine should allow deployment of the workflows themselves as microservices.
   6) The engine should support persistence of workflow, workflow state and should allow stop and re-starting of workflows.
   7) The engine should use standard databases/data stores for persistence.
   8) The engine should provide an audit log for logging the activities of the workflows.
   9) A workflow system should provide a monitoring tool with a web-based GUI that:
      i. Monitor the status of workflows,
      ii. Enable start, stop of workflows,
      iii. Track resource utilization of the runtime engines,
      iv. Monitor health of the runtime engines,
      v. Set/change log levels,
      vi. Change configuration parameters of the workflow engine without shutting down the engine
      vii. backup, archive the persistent store

d. All the GUIs of the system should be accessible from standard browsers – Chrome, Firefox, Safari. Support for each of these browsers should include the latest stable version and the version immediately before that.

e. The workflow system and all its components should be capable of being deployed in virtual machines or a container.

f. The monitoring tool should have role based secure access for different category of users of the tool.

g. The SI should ensure that the use cases for the workflow engine meet the throughput, concurrency and response times of the respective use cases.

h. The workflow engine should be deployed across multiple DCs and should support the RPO and RTO of Philsys.

i. The SI must customize the tool as per PhilSys use case requirements.

j. The SI must create/modify/customize the required workflows and integrate with all the relevant applications/microservices.

7.4.4 Customer Relationship Management System (CRMS)

a. The SI MUST design, develop, test, install and maintain the CRMS.

b. The CRMS MUST centralize all incidents and complaints from both members of the public and PSA partners and track them using dedicated unique identifiers.

c. The CRMS MUST include a web application including a set of GUIs and tools for PSA operators to efficiently process incoming requests.

d. The SI MUST integrate the CRMS with all relevant PhilSys Information System such as the IDMS, the IAM (operators' login) and the NS (for sending updates to claimants via SMS).

e. The CRMS MUST support complaints by members of the public as well as PSA partners through the following communication channels:

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

f. The CRMS MUST timestamp all transactions and automatically prioritize them based on the distance with the relevant KPIs of the SLA.

g. The CRMS MUST keep a history of all transactions not limited to metadata, but including identifiers, timestamps and content of all exchanges.

h. The SI MUST include all data processed and generated by the CRMS into the PhilSys backup scope and policies.

i. The CRMS MUST produce and disseminate activity reports on a daily, weekly, monthly, quarterly and yearly basis.

7.4.4.1 Customer Relationship Management

a. The PhilSys Information System will require an inbound Call Center. The Call Center shall act as a citizen and ecosystem partner application and provide resolution of queries of residents and ecosystem Partners regarding PhilSys services such as, Registration services, Authentication services, TSP and RP related queries, etc.

b. SI shall be responsible to setup the call center.

c. The SI shall be responsible to procure, supply and maintain the required IT/ Non-IT infrastructure (Hardware/ Software) for the operations of the call center.

d. The SI shall provide for a National toll-free number at the National Call Center with sufficient number of lines for logging of calls.

e. The SI should assign **a National Call Center Manager** for managing the CRMS. The National Call Center Manager would be responsible for handling escalations from all locations and appraise PSA on daily basis. The National Call Center Manager should be **onsite and assigned on a full-time basis.**

f. The SI shall:

   1) provide a toll-free number for the Call Center and will bear the operational cost of this number.

   2) provide physical space for the call center along with necessary Electrical (Power Supply, Wiring, Power Sockets, Lights, etc.) and Physical Infrastructure (Tables, Chairs, etc.);

   3) provide necessary IT (Hardware, Software, Network) and Non-IT Infrastructure (Communication Equipment such as EPBX, IVR, Dialer, Telephones, Headsets, etc.);

   4) be responsible for supplying and implementing a Customer Relationship Management System (CRMS) to support Call Center Agents;

   5) be required to maintain the infrastructure provided at the Call Center covering the period of the entire contract.

   6) provide necessary manpower i.e. supervisors and call center agents to run the Call Center.

   7) be responsible to train the aforementioned manpower for the resolution of citizen and partner queries.

   8) be responsible for ensuring that the infrastructure provided is operational from 8 AM – 6 PM from Monday to Saturday excluding government holidays.

g. The call center will provide support in both English and Filipino languages.

7.4.4.2 Deployment of CRMS Solution for Call Center Operations

Scope of work for deployment of CRMS solution includes the following:

7.4.4.2.1 Deployment of Infrastructure for Call Center Operations

a. The SI shall provide PRI lines and a toll-free number for the Call Center and will bear the operational costs of these items.

b. The SI shall provide physical space for the call center along with necessary Electrical and Physical Infrastructure as follows:

   1) Premises & Furniture
   2) Required floor space
   3) Lighting
   4) Basic amenities e.g. water facilities
   5) Power connection
   6) Standard fire-fighting systems
   7) Cubicles, chairs, cabinets, etc. constructed / provided to suit a typical Call Center
   8) Network Connectivity between National Call Center and DC, and National Call Center and DR

c. SI should ensure that the call center has requisite IT and other Infrastructure to support the project requirements. SI shall be required to provide and maintain all IT and Non-IT infrastructure (excluding only those items mentioned in points given above) required for successful operations of the Call center include, but are not limited to, the following:

   1) Hardware such as desktop/laptops with headsets, telephones, etc.
   2) Software such as CRMS, Computer Telephony Interface connector to integrate CRMS and IVR, call barging and recording software, etc.
   3) Communication Equipment such as IVR, Dialer, EPBX, etc.
   4) Automatic Call Distributor (ACD) for distribution of incoming calls to Call Center staff as they are received. SI shall be responsible for installation of the ACD. ACD should have at least the following features:

      - System should be able to intelligently route the callers to Call Center staff based on their availability to take calls on first come first serve basis.
      - Standard features like Call Transfer, Conference, Barge-in, Dialled Number Identification Sequence (DNIS), Automatic Number Identification (ANI), and Caller Line Identification (CLI) etc.

- System should announce the queue waiting time for the caller before getting attended by a Call Center
- System shall support the ability to play customized announcements per queue as defined by the administration.

d. SI will be responsible to integrate the infrastructure provided by PSA with infrastructure provided by SI to make the call center operational

7.4.4.2.2 Other Responsibilities of SI for Call Center Operations

a. Preparing a detailed plan for setting up of Call Center Operations with timelines and activities and submitting the same for PSA's approval

b. Training is an important aspect of the Call Center agents. The SI should impart proper training in soft skills like call handling, exposure to related applications etc. so as to prepare the customer service executives to attend to incoming calls effectively. SI shall also prepare the required training material

c. SI shall prepare standard operating procedures of call center including call handling processes, quality assurance and escalation management

d. SI will extend all the required support to PSA during their Random or Regular audits of the call center operations and call center facilities.

e. Disaster Recovery and Business Continuity: The SI shall ensure proper procedures are established for Call Center systems in the event of a disaster to protect and ensure continuation of Call Center services.

7.4.4.3 Reporting

a. SI should generate standard reports to measure/verify various service level(s), to monitor the performance of agents, etc.

b. SI shall prepare and submit reports to PSA as per the mutually agreed reporting structure. These reports shall include but are not limited to the following:

1) Incident, devices and system logs/ security logs (category, severity and status of call etc.)
2) Incidents escalated
3) SLA compliance/non-compliance report
4) Problem Management
5) Key learning from similar previous experience

6) Escalation procedure for handling significant issues

7) Call Center staffing

c. The SI and PSA will mutually agree on the format of the reports to be submitted by the SI to PSA. The SI must provide at minimum the following reports: (See also Annex I for other reports)

1) Reports based on time period

2) Type of Complaints/queries/demand/analysis

3) Repeat request or complaints analysis

4) Call waiting time

5) Lost calls

6) Call time (Average Talk Time/Hold Time/Handle Time)

7) Hourly call details

8) Complaints pending for more than defined time period

9) Calls Handled

10) Abandoned Call Rate

11) Delay Before Abandon (Average/Longest)

12) Staffing related Report

13) Other monthly MIS, SLA reports, number of agents logged in

7.4.4.4 Monitoring

a. SI should extend all the required support to PSA team for monitoring and access to all subsystems and records pertaining to call center operations for PSA

b. SI shall be responsible to assist the PSA officials in monitoring of the call center agents and operations

7.4.4.5 Key Features of the Proposed Call Center

The key features of the proposed Call Center are given in the table below:

Table 43. Key Features of Call Center

Description / Activity	Remarks
National Call Center	Phase-1: 10 seats

	Phase-2: 20 seats
Languages supported	English and Filipino
Operations	6 days a week (Monday – Saturday) 8:00 AM to 6:00 PM
Accessibility	Accessible through a Toll-Free Number, IVR Solution Support processing of complaints coursed through the communication channels specified in Section 7.4.4 (e)
Quarterly Review	Half-Yearly review of call volumes and number of seats required to provide services
Offsite/Onsite	Onsite at premises of PSA

An illustrative list of queries and complaints that may be posted with the PhilSys Call Center is given in Section below to assist the bidder in understanding the nature of support to be provided using the CRMS solution.

7.4.4.6 Sample Queries at the Call Center

An illustrative list of queries and complaints that may be posted with the PhilSys Call Center is given below to assist the bidder in understanding the nature of support to be provided using the CRMS solution.

Table 44. Indicative types of Queries at a Call Center

Queries (Sample)	Queries (Sample)
General – Queries/Complaints of Resident for Registration • Where can I register • How to book an appointment • Can I reschedule the appointment? • What documents are required for registration / update • Are there any fees for registration / update? • What is the status of my registration? • My registration has been rejected, what should I do • How to update my demographic details • How to update my biometric details • At what age, can my child register	General – Queries/Complaints of Ecosystem Partner • I want to register myself as TSP / UA • What is the application procedure, timelines and documents required? • Whom do I contact for Registration? • Authentications are not working • eKYC is not working • OTP is not being received • Which authentication devices should I use? • What is the procedure for registration of authentication devices? • What is PCN, can I use it

Queries (Sample)	Queries (Sample)
• I do not have birth certificate, what should I do • Do I need to take pre-Registration slip for registration? • I have lost my pre-Registration slip, what can I do	
General – Queries/Complaints of Registration Officers • I am unable to login • I am unable to download pre-Registration information • My registration software is not working • My registration kit is not working • I cannot upload the registration packet • My registration software is not allowing me to register more residents • I am unable to capture biometrics • What to do when resident has problem with quality of biometrics or missing fingers	General – Queries/Complaints of Residents for Authentication • How can I generate my Electronic ID? • How can I lock/unlock my biometric? • Can I change my PSN? • I have lost my PSN and I cannot authenticate • I cannot authenticate despite repeated attempts • I have received an alert of authentication / eKYC

7.4.5 Business Intelligence and Analytics System (BIAS)

PSA is seeking the capability to analyze large quantities of data, transform the data into intelligence and insight, and deliver this intelligence and insight to the PSAs processes and users. The KPIs need to be viewed from a Function, Process and Users' perspective. The PSA believes that data mining and statistical analysis is a key requirement for Planning and Dashboard for PhilSys Information System.

a. The SI's scope of work includes procuring, commissioning, configuration, implementation, integration, deployment, and maintenance of an enterprise level Business Intelligence and Analytics System for PhilSys.

b. The SI shall carry out a detailed requirement phase upon award of the contract to review the data analytics requirements for the Data Analytics module.

c. The SI shall produce a detailed functional specifications and design specifications, including detailing the data analytics module to be developed, system architecture design, design principles / considerations, etc.

d. SI shall create a data lake to host and manage the large amount of data – both structured and unstructured.

e. The SI shall enable the system to provide comprehensive monitoring of registration and authentication through Business Intelligence (Dashboards and Reports) and Analytics. The mechanism would also allow for alerts, reminders, etc. to be sent through a unified dashboard.

f. Regarding BIAS, the SI shall also perform the following:

    1) Propose, design and implement an integrated BIAS
    2) Quality assurance test for BIAS
    3) Provide documentation for BIAS
    4) Perform integration with internal systems' data sources for BIAS
    5) Master Data Management for all applications

g. The proposed product should preferably be an open source solution along with Enterprise support.

h. The solution must have analytics and dynamic reporting. Reports should allow for exportable format such as pdf, excel, html etc.

i. The SI should propose tools that allow customizable reports. The generation of the report shall not impair system performance.

j. PSA shall prescribe reports to be developed which will be identified at requirements stage as well as operations phase.

k. The BIAS should allow PSA to customize notification of certain indicator that PSA is interested to trigger activities / actions. The BIAS should have a user interface to extract data based on the data required for self-analytics and report generation. The BIAS should also allow for ad-hoc queries pertaining to the module for quick access to real time information and allow users to define filters or parameters to view the data from different perspectives.

l. SI has to prepare detailed requirements around reports and study PhilSys KPIs to define required reports, analytics capability to meet the needs of PhilSys Information System.

m. The scheduled (weekly, fortnightly, monthly, quarterly, yearly) reports need to be extracted based on the agreed format and submitted to the PSA for KPI tracking purposes.

n. A key feature envisaged as part of BIAS for PhilSys is fraud analysis.

o. Proposed BIAS must allow for the Design and distribution of dynamic, interactive reports and dashboards using a drag-and-drop designer environment which includes but not limited to:

    1) Auto-charting automatically choose the best graph suited to display the selected data
    2) Variety of analytical visualization such as line, bar and pie graphs, box plots, animated bubble plots, correlation matrices, forecast reports, etc.

p. Embeds Artificial Intelligence/Machine Learning into the platform and allow for automated analysis of available variables.

q. Use predictive analytics to analyze the data and predict the possible outcomes, forecasts etc.

r. Includes geospatial analysis, network diagrams, ability to create calculated, aggregated or derived data items

s. Able to allow for the reuse and sharing of reports, including filters, calculations, hierarchies and report element formatting

t. Must be scalable and includes the handling of ever-growing numbers of users, data types, data volumes, and the evolving range of BI and analytical work loads

u. Ability to create alerts for a report object so that subscribers are notified via email or a text message when the threshold condition is met

v. Ability to provide self-service analytics that includes the creation of drillable hierarchies in a self-service manner without the need to predefine user paths and network diagrams to determine data links

w. Availability of a unified platform that allows users to customize its whole analytical journey. Ability to perform powerful analytic insights without writing any code or choosing to use the graphical user interface or choosing to integrate other technologies into the platform, like open source coding and APIs

x. Availability of a collaborative platform that allows different users to perform different tasks in one platform such as managing and preparing data, visualize and create dashboards, build models, performing AI and other tasks in one application under one unified and collaborative platform without leaving the browser.

y. The tool should provide role-based access to various users of the system

z. All access to be system shall be via a secure web-based portal

aa. The middleware, data stores used by the tool should be a standard COTS/Open Source product – should not use any proprietary components

bb. The tools should be deployed as virtual machines or containers on the proposed hardware platform (x86 based).

7.4.6 Document Management System (DMS)

a. The SI MUST develop or customize, test, install and maintain the DMS.

b. For this particular system, the SI can either purchase and customize a COTS software product

c. The DMS MUST support all functions listed in Sections 6.3.2.2 Registration Procedure and 6.3.3 Updating Process. Notably, the DMS MUST allow for the storage of all scanned documents submitted by applicants during pre-Registration, Registration and personal data update.

d. Document management system should be interoperable and follow open standards to facilitate smooth takeover by any other vendor appointed by PSA.

e. The DMS should be integrated with pre-registration applications, registration, IDMS, KMS and LMS.

f. In addition, the SI shall allow at least ten (10) internal users to connect directly to the DMS application.

7.4.7 Partners and Devices Management System (PDMS)

For authentication service delivery, a federated model is to be adopted. In this federated model, there will be agencies which will be connected directly to the PhilSys through secure and dedicated network. These agencies will be known as Trusted Service Providers (TSP) and will be responsible for extending the services to other agencies. In addition, there will be agencies that will utilize the authentication services in their operations and process. These agencies known as Relying Parties (RPs), will submit the request for authentication services to PhilSys through TSP. The RP will deploy the biometric capture devices at their point of services and these biometric devices will have to be pre-registered with the PhilSys. The devices so authorized after the registration will be known as 'Registered Devices'.

The SI MUST design, develop, test, install and maintain the PDMS that will be used to centrally manage the following aspects:

a. **On-boarding of Trusted Service Provider**: On-boarding the TSP which involves administrative procedures, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.

b. **On-boarding of Relying Parties**: On-boarding the RPs which involves administrative procedure, technical integration support, compliance audit, maintenance of secure keys for data exchange, etc.

c. **Registration of Devices**: Maintaining and updating the list of registered devices for all the RPs.

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

7.4.7.1 Devices Management Server

The SI will implement the Management server /client only for registration devices which can be an independent module outside of PhilSys system. The SI will work with the device provider to define the

communication protocols and API's between the MDS (software component provided by the device provider to make it compliant with MOSIP device specifications) and the Management Server/Client for registration devices. The SI will support the device vendor for the development of the Management client functionality to communicate with the management server/client, testing and deployment for registration devices. SI will also provide O&M for this server along with other components of the PhilSys Information System. (Details on the management server/client for registration devices functionality and interactions with MDS is available at **https://docs.mosip.io/platform/functionalities/biometric /mosip-device-service-specification#management-server-and-management-client**)

- Validate the devices to ensure its a genuine device from the respective device provider. This can be achieved using the device info and the certificates for the Foundational Trust Module.

- Register the genuine device with the PhilSys device server in the PDMS system.

- Manage/Sync time between the end device and the management server. The time to be synced should be the only trusted time accepted by the device.

- Issue commands to the end device for

    1. De-registration of the device (Device Keys)
    2. Collect device information to maintain, manage, support and upgrade a device remotely.

- A central repository of all the approved devices for the PhilSys Information System.

- Safe storage of keys using HSM FIPS 140-2 Level 3. These keys are used to issue the device certificate upon registration and rotate these keys periodically as per configured frequency.

- Should have the ability to push updates from the server to the client devices.

T OBJ OBJ

7.4.7.2 Relying Parties Management

7.4.7.2.1 Enablement of Partners for Authentication Services

The key activities of SI with respect to the authentication services TSP partner on-boarding would involve the following:

a. Provide handholding and guidance to the Relying Parties in order to enable them to setup adequate facilities and IT infrastructure for leveraging authentication services.

b. Drafting of sample Memorandum of Understanding (MoUs) for the authentication service partner i.e. TSP and RP. The MoUs should set the expectations and intentions of both the

parties for collaboration and for facilitation of subsequent agreements and documents for working with PhilSys.

c. Create documents related to standards, processes and procedures to help PhilSys officials and RPs for the on-boarding.

d. Providing relevant Application Programming Interfaces (APIs) and technical support.

e. Addressing and resolving of any queries and concerns pertaining to on-boarding by the RPs.

f. Facilitating the certification of biometric devices on make, model and specifications and making the details available on the relevant portal for the RPs.

g. Providing relevant reports to PhilSys officials through PhilSys Information System to ensure a consolidated, single-view, integrated reporting of performance of the authentication service partners.

7.4.7.2.2 Authentication Services Management

a. PSN-based authentication services would be one of the main services of PhilSys Information System. It is expected that PSA would appoint TSP and Relying Parties (RP) in the Philippines for PSN based authentication services. **It is expected that the PSA and its nominated agency would be one of the first TSP and RP for using authentication services**. This section outlines key responsibilities of the SI for authentication services management and providing support to RP.

b. SI Shall be responsible for developing the PSN - Authentication Services Implementation Framework (PSN-ASIF) which will be a document comprising set of standards, processes, protocols, privacy and liability policies, trust models, enforcement mechanisms and specification of authentication devices. The various entities involved in PSN-ASIF are:

   1) Citizens and Resident Aliens of Philippines - Beneficiaries who have been issued a PSN and need to authenticate in order to avail a service.

   2) Registered Devices – devices employed by the TSP and RP in both the government and the private domains. Examples could include micro-ATMs, POS devices etc. These devices would have to be registered by the SI.

   3) Intermediaries – In future the PhilSys Information System may engage with the Intermediaries. SI shall be responsible for designing the processes and protocols to integrate the Intermediaries into PhilSys Information System.

   4) Relying Parties (RP) – An organization or entity connecting through TSPs for PSN-based authentication/eKYC. These may be Government Departments and Agencies, Private Sectors, etc.

   5) Trusted Service Provider (TSP) – Entities proposed to be engaged that shall provide authentication services to various RPs.

c. The SI shall be responsible for the following:

1) Manage the authentication activation request from respective TSPs and RPs. SI shall be responsible for performing all necessary coordination with the respective RP to ensure that the authentication activation request is completed in a timely fashion.
2) In case PSA decides to make authentication services a paid service, the revenue generated from such services shall be electronically collected through a payment gateway. The SI shall provide payment and billing system.
3) Collection, billing and accounting of authentication fees shall be undertaken by the PSA as per the rules of Government of the Philippines. The process, role and responsibility of SI in this regard will be finalized in consultation with PSA.
4) PSA may appoint more than one service provider called as the "Trusted Service Provider" (TSP) with authentication services in different geographical areas.
5) SI shall be responsible for the management of IDs of TSPs and RPs, registration of authentication devices and accessing PhilSys Registry including managing addresses, email ID, telephone numbers and other contact information of TSPs and RPs.
6) SI shall prepare detailed security architecture for the authentication services and implement the same.

7.4.7.2.3 TSP Authentication System (TSPAS)

a. **The SI MUST design, develop or customize, test, install and maintain the TSPAS.**
b. The TSPAS MUST support all functions described in *Section 6.4.3.10* Trusted Service Provider Authentication System (TSPAS)
c. The SI MUST design, develop and ensure application-level security for the TSPAS.

Error! Reference source not found.Error! Reference source not found.

7.4.7.2.4 RP Authentication System (RPAS) Sample Application Development

a. The PSA plans to rollout a sample application for reading biometrics from biometric devices, to send authentication / eKYC request by the PhilSys and to receive & display the authentication response / eKYC provided by the PhilSys. Please note that this pilot application will not be massively rolled out (the RPs will develop their own client software, implementing the authentication API) **. In the pilot project for two (2) Relying Parties, there will be two (2) priority use cases:**
    1) PSA Civil Registry
    2) DSWD Beneficiaries for *Listahanan* Registry and the *Pantawid Pamilya* ID[9]

[9] DWSD Listahanan and 4Ps ID program are listed as potential priority use cases. The PSA will confirm with the Winning Bidder on the final list of participants for the PSN-ASIF framework to be developed by the SI

b. In this regard, the SI MUST design, develop and install the RPAS user application in which the user can perform the following tasks:

   1) Enter the PSN, select the desired service (authentication or eKYC), then select the guide (demographic, fingerprint, iris, face, OTP or a combination of both).

   2) The beneficiary may provide information (demographic, biometric OTP or combined) to request authentication / eKYC

   3) The web interface will be integrated into the user application for the submission of the application authentication / eKYC and receiving the response

   4) The web interface will be able to view the response received from the TSP. A Web interface is to be developed for the indicated platforms (.Net, Java and PHP).

c. The RPAS MUST be compatible with all biometric scanners certified by PSA

d. The SI is required to propose a Multi-Protocol Label Switching (MPLS) router for the two RPs identified above. These RPs will be connected to the PhilSys platform via a dedicated MPLS cloud or VPN.

e. The SI shall provide extended support in the set-up of two (2) priority use cases.

7.4.8 Fraud Detection and Management System (FDMS)

a. The SI MUST design, develop, test, install and maintain the FDMS that will analyze all business and technical transactions processed by the PhilSys (including but not limited to registrations and authentications), detect potentially fraudulent cases and either block transactions or allow PSA operators to investigate the same.

b. For this particular system, the SI can either purchase and customize a COTS software or deploy an open source product.

c. The FDMS MUST be based on a set of configurable business rules. The FDMS MUST feature one or more configurable, rule-based fraud detection engine(s).

d. The FDMS MUST automatically lock authentications / eKYC for a given registered person in some known contexts (e.g. selected proven fraud cases).

e. The FDMS MUST flag transactions forwarded by the MVS for investigation. The SI MUST interface the FDMS with the MVS to that end.

f. The FDMS MUST leverage advanced technology such as fuzzy matching and graph representations to detect abnormal activity.

g. The FDMS MUST monitor all PhilSys transactions related to authentication transactions, manual adjudication and manual verification.

h. **Operational Integrity during Registrations and Verification**; Should be able to flag and/or address certain scenarios such as:

1) Registration officer has direct link with citizen – e.g. has same address or other details as Applicant.

2) Registration Officer linked to 'high risk' registrations – e.g. Registration Officer processing unusually high ratio of Applicants with high-risk scores or low biometric scores during capture.

i. **FDMS Data Management Requirements**

1) Should provide single platform for data management requirements such as profiling, extraction, cleansing, standardization, parsing, casing and data matching.

2) Can do extensive and out of the box profiling of data in existing database.

3) Has the ability to present profiling results in textual report format.

4) Has the ability to present results in graphical formats and allow users to easily share profiling results and scorecards.

5) The solution can integrate to virtually any type of data source (or provide an alternative solution to capture data), fuse the data together, and enrich content so that it's ready for searching and analysis.

6) Has the ability to develop and deploy data quality monitoring rules to proactively alert users of occurrence of bad data. Alerts can also be sent through email notifications or other available alert functionalities of the proposed solution.

7) Has the capability to configure multiple fields and weighting of each field to get an overall match score. The threshold for automatic consolidation must also be configurable.

8) Capability to modify packaged data quality rules.

9) Should have an open data model to meet different and evolving business requirements and situations.

10) Must be able to do on-demand integration and blending from structure, unstructured or semi structured data sources.

11) Must be able to auto-generate data transformation templates at runtime with metadata injection.

12) Must have an integrated platform for data orchestration and transformation.

13) Database connection can easily be done in an interactive GUI (as much as possible direct SQL coding is not required).

14) On connectivity and data access, include a requirement that connects to virtually any data – big data or streaming, across various hardware environment with Ready-to-use analytical transformations, including correlations and frequencies, distribution analysis and summary statistics.

15) On connectivity and data access, include a requirement that provides for a powerful, easy-to-use transformation user interface that supports collaboration, reuse of processes and common metadata.

16) On data management, include a requirement that provides mapping technologies that can easily propagate column definitions from sources to targets and create automated, intelligent table joins and facilitates reuse of existing table definitions and business rules

17) On data cleansing, include a requirement that embeds data quality into batch, near-real-time and real-time processes

18) On data cleansing, include a requirement for an interactive GUI interface that enables profiling of operational data to identify incomplete, inaccurate or ambiguous data

19) On managing data processes, Build and edit data management processes with a visual, end-to-end event designer that allows control over the execution of data integration, data processes and data quality jobs

20) On metadata management, include a requirement that provides for a complete and shared metadata environment that enables consistent data definition across all data sources and has the ability to determine the path, processes and transformations taken to produce the resulting information

21) On data standardization, include a requirement of an Out-of-the-box standardization rules that conform data to your corporate standards, or allows customized rules for specific situations

22) On querying, provide consistent business views across all data sources with optimized query processing that provides instant access to information.

23) Identify, standardize and correct master data by each transaction, in hundreds of transactions at a time or in a single pass of the source data.

24) On data integrity, include a requirement that provides features such as semantic data descriptions and sophisticated fuzzy matching, you can check and control data integrity within a web-based reference management interface.

25) On data governance, implement business rules and policies across the enterprise to ensure compliance. These actions can be tracked and monitored across the entire governed environment.

7.4.8.1 Real-Time Fraud Detection

a. The FDMS MUST provide real-time fraud detection services by parsing the PhilSys logs and interfacing the Authentication Management System.

b. The FDMS MUST be able to automatically detect abnormal registration and authentication patterns such as but not limited to:

1) Suspicious behaviours (e.g. replay attacks)
2) Multiple operations of same or similar nature conducted in a limited timeframe originating from the same user and / or registration kit or Relying Party
3) Operations carried out outside of normal business hours

c. **Verification Integrity through Risk Assessment Engine**

1) Provide real-time risk score and reason code during registration/authentication.
2) Must include an Investigation System that will proactively issue alerts for triage and investigation & disposition to watch list.
3) Risk Assessment Engine must be triggered during biometric authentication at relying parties.

7.4.8.2 Non-Real Time Fraud Detection

a. The FDMS MUST feature automated non-real time (ex. Batch processing of transactions) detection of potential fraud cases.

b. The FDMS MUST feature an Extract Transform Load (ETL) tool and a dedicated data warehouse and connect to all relevant audit trails generated by the various PhilSys systems (e.g. from the IDMS for registrations and from the AMS for authentications).

c. **Investigation System Requirements**

1) Able to generate alerts after analyzing batch-based data
2) Scores using hybrid & link analysis
3) Ad-hoc queries / cases for whistleblowing & citizen interviews

7.4.9 Enterprise Management System (EMS)

a. The SI MUST test, install and maintain the EMS.

b. The EMS MUST include the following features:

   1) Monitoring of all critical IT infrastructures including software applications, storage systems, servers, networks using SNMP or any Standard Management Protocols

   2) Monitoring of backups

   3) Incidents management

   4) Automated correlation of events

   5) SLA management including edition of reports

7.4.10 Identity and Access Management System (IAMS)

a. The SI MUST design, develop or customize, test, install and maintain the IAMS.

b. For this particular system, the SI can either purchase and customize a COTS or customize its own product.

c. The IAMS MUST maintain a centralized directory of all PhilSys users that will be used by all PhilSys applications for logical access control and access rights.

d. The IAMS MUST be the sole authoritative source for centrally managing logical access to all PhilSys Information System.

e. The SI MUST integrate the IAMS with all PhilSys Information System.

   1) The IAMS should be integrated with the Enterprise Directory (AD, LDAP).
   2) Should support open standards like XAML , O_AUTH
   3) The IAMS should provide a Single Sign-On feature.

f. The SI MUST integrate the IAMS with the proposed solution for PhilSys operators' login.

g. The IAMS MUST allow an authorized user to manage PhilSys users throughout their lifecycle and configure his / her access rights for each PhilSys application (fine granularity configuration of access rights at PhilSys application level).

h. The IAMS MUST feature the management of MFA (Multi-Factor Authentication) The IAMS MUST include measures to ensure that authorised users (e.g. operators) are authenticated securely and that risks such as biometric spoofing or credential sharing are mitigated. The IAMS should ensure that the highest level of security / accountability is maintained (e.g. non-repudiation).

i. The IAMS MUST allow an authorized user to manage the provisioning of such individual physical tokens throughout their lifecycle.

j. The IAMS MUST offer ergonomic GUIs for doing so.

k. The IAMS MUST log all transactions (including granular changes brought to access rights).

7.4.11 Card Personalization and Management System (CPMS)

Card Personalization will be used in Card Printing and Management facility of the PhilSys, it has the following features:

a. The SI MUST develop, test, install and maintain the Card Personalization and Management System (CPMS).

b. For this system, the SI can either purchase and customize a COTS software product or develop a bespoke application.

c. The CPMS MUST generate, forward and follow up on PhilID Cards personalization orders.

d. The CPMS MUST print the PhilID Cards.

e. The CPMS MUST publish a "get current status" service via its API so that any other PhilSys Information System can get the status of a given PhilID Card at any point in time.

f. The CPMS must be able to perform Quality Assurance (QA) test on personalized PhilID Card.

g. The data for printing shall be provided by both pull and push mechanism to the BSP Service Provider in Unicode XML (Extensible Markup Language) / or JSON file format or an equivalent electronic format as specified by PSA.

h. The Network Connectivity and bandwidth of the lease line shall be provided by PSA and it would be capable of transferring electronic data, equivalent to the day's volume.

i. The data transfer shall be on SFTP (Secure File Transfer Protocol). The SFTP download / upload client shall be provided or specified, as the case may be, by SI to the BSP Service Provider and the SI shall install the server with the same SFTP client at BSP printing premises and use it for download / upload of data from / to PSA. The installed SFTP client shall be used exclusively for PhilSys work.

j. The SI using HSM will digitally encrypt the data / file to be sent to BSP Service Provider. The Digital Certificate / HSM required for data encryption will be procured by the SI and its public key shared with PSA

k. The Transaction Reference Number that has been provided on the registration phase will be printed on every cover letter.

l. The SI shall deploy defensive check mechanisms for verifying the integrity of data received from PhilSys Registry. The SI is expected to validate the data file structure, verify the mandatory fields as specified by PSA and print only unique records. The verified error records are assigned a reason, skipped (not processed for printing) and written to the skipped file thereby creating a report for all the records skipped for printing. SI shall provide the list of reasons for skipping records to the PSA. The report for such skipped file is to be prepared and submitted to PSA on periodic basis.

7.4.12 Card Management System (CMS)

a. The CMS is used by the PFRC to provide services to clients such as request for card replacement, information on status of card replacement, card releasing and card delivery status.

b. The SI MUST develop, test, install and maintain the Card Management System (CMS).

c. For this system, the SI can purchase and customize a COTS software product

d. The CMS MUST interface with PhilSys Web Portal and PhilSys Mobile Application.

e. The SI shall be responsible for the development of API's to fetch the tracking data from the systems of the PhilSys Delivery Partner to the PhilSys Fixed Registration Centers, Call Center, Mobile Application and PhilSys Web Portal.

7.4.13 Card Batching Utility (CBU)

a. The CBU is a utility that retrieves the records from the PhilSys Registry that are due for card printing, prepares print files containing PCN, demographic information, front facing photograph and QR Code (with embedded metadata) of newly registered records, card reprinting or card replacement. The CBU batches the print files and forwards these to CPMS through the CWE.

b. The SI MUST develop, test, install and maintain the Card Batching Utility. The CPMS sends requests for batches of records for card printing to the CBU.

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

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

e. The QR code contains the registered person's PCN, name and other demographic information printed on the card, low-resolution photo, and two best fingerprints' labels.

f. The SI shall develop the procedure to generate the labels for the two best fingerprints from the registration packet.

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

h. The CBU MUST interface with the CPMS, CWE and IDMS.

i. The CBU MUST digitally sign all data stored in the QR code and include the digital signature in the same QR code for verification purpose.

7.4.14 Knowledge Management & Learning Management System

7.4.14.1 Knowledge Management System (KMS)

The SI is expected to consider the following while designing the Knowledge Management System as part of PhilSys Information System.

a. SI shall be responsible for supply, design, develop and maintain the Knowledge Management System

b. The Knowledge Management System must be designed in a flexible manner so that additional categorization fields can be added in the future, as and when required. Also, the system should be able to handle knowledge of any form, including different subjects, structures and media.

c. All capabilities should be available on a web application accessible on mobile smartphones as well as desktops / laptops.

d. The Knowledge Management System should capture metadata when adding a document such as keywords, date, title, description, target audience, date of issue, date of expiry etc.

e. SI shall be responsible for uploading all the training material prepared for trainings in KMS

f. SI shall be required to prepare a comprehensive frequently asked questions (FAQs) and upload them on the KMS.

g. For this particular system, the SI can either purchase and customize a COTS software product.

h. The KMS MUST allow to store, search, display and share internal documents.

i. Knowledge Management System should be integrated with the PhilSys Web Portal and Document Management System.

7.4.14.2 Learning Management System (LMS)

The Learning Management System would handle training and knowledge transfer of various stakeholders from Registration Officers to internal 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 key features of the Learning Management System are as follows:

a. **Training Need Analysis**: The LMS must have the capability to capture training needs of different types of users for analysis and development of new trainings

b. **Training Monitoring**: The LMS should have the capability to monitor trainings completed by different users and sending reminders to users for completing the registered trainings especially mandatory trainings.

c. **Training Feedback Mechanism**: The LMS should have the capability to capture feedback of trainings from Trainees for continuous improvements in training.

d. **Training Schedules**: The LMS should have the capability to publish a detailed training schedule.

e. **Audio Visual Trainings**: The LMS is also required to provide Audio-Visual Trainings to the users for assistance in operating / navigating through different applications. The modules/ section wise training material, especially in the form of Audio-Visual content or animation, apart from PDF version, have to be uploaded in each module/sub-module/section of the PhilSys Portal which can be played at any given point of time through the browser. The users should find it easy to understand the process and functionality better by seeing the audio-visual training content for that specific module/sub-module/section and work accordingly as required.

f. **Training Navigational Capabilities**: These Audio-Visual clips will have the functionality to start, stop, pause, back and forward options, so that the user can play the training content as per his own free will and requirement. All these specific module / sub-module / section wise audio-visual training content should be integrated to form a complete training of the Portal, and uploaded on the portal free access, download and ready reference.

g. **Online Help / Reference with Search option**: It is also proposed that the training contents and user manuals will be made available to users in downloadable (PDF) format so that the users may refer / download it for their own personal reference as and when needed.

h. **Language Support**: Trainings material would be available in English.

7.4.15 Notification System (NS)

7.4.15.1 SMS Gateway and Services

a. PhilSys shall be enabled to send and receive SMS based notifications primarily for sending alerts to users (officials, beneficiaries).

b. Outbound SMS shall be automated based on an event or time during service life cycle. For example, upon successful generation of a PSN number, registered beneficiary shall receive an SMS notification providing the PSN number.

c. The SI must use the SMS gateway provided by PSA or its appointed party and integrate this gateway with PhilSys to enable outbound SMS services.

d. The cost of SMS charges shall be borne by the PSA.

e. One-time integration cost for SMS gateway shall be borne by SI.

f. The SMS application will expose an API to initiate the SMS broadcasting or alert notification.

g. The SMS service should support USSD codes.

h. Support automated alerts that allows to set up triggers that will automatically send out reminders.

i. Include provision to resend the SMS in case of failure of the message.

j. Must have common features like non-acceptance of landline numbers, unacceptable mobile numbers etc.

k. Should automatically create a log of SMS sent.

l. The message shall be sent through command line interface/API and/or Web Interface.

m. The SMS service shall provide standard reports like success/failure report on current as well as historical / cumulative basis.

n. The SI shall prepare a draft SMS content and obtain approval from the PSA on the SMS content before rolling out the SMS services.

7.4.15.2 Email Gateway

a. Email services are envisaged to be made available as part of the PhilSys solution design to send alerts / intimations / automated messages to registered email ids, based on the preferences set up / opted by individual resident.

b. An authenticated SMTP mail service (also known as SMTP relay or smart host) is envisaged to be integrated with the solution for sending mail from the solution and delivered to the intended inbox. Support anti-spam features. The SI must consider this service and its integration in the proposal.

c. The SI is required to propose email solution such that there is one email address per user. Additionally, the email address will be created for applications (e.g. authentication.notification@psa.gov.ph). For such cases, 100 email addresses will be required.

7.4.16 Payment and Billing Solutions

7.4.16.1 Requirements for Payment Solution

a. The SI is required develop a payment solution to allow various stakeholders and residents to make payments for PhilSys services.

b. The SI is required to integrate the system with Payment Gateway to enable online payment for various PhilSys services by citizens / residents.

c. The payment system shall capture the purpose of payment, details of the user and calculate fee based on configurable business rules.

d. The system shall be designed such that business rules to calculate the fee based on the type of application can be created in the system using a business rules engine and which can be triggered at different points in the application workflow.

e. The system shall allow payment to be dynamically updated based on changes to inputs in the application workflow using a simple user interface – e.g. during the application processing, if an authorized person decides to waive the fee for the request, the payment module should be skipped.

f. The system shall support multiple payment options such as cash, Point of Sale ('PoS'), Credit and Debit cards and other modes of electronic payment via wallets, payment interfaces of banks, etc.

g. The system shall support multiple payment gateway providers and payment gateway devices.

h. The system shall record an audit trail of all actions performed using it and should be able to generate audit logs and activity reports.

i. The system shall support payment refund and payment status tracking.

7.4.16.2 Requirements for Billing Solution

a. PSA requires a Billing Solution to support billing of various authentication and eKYC Relying Parties as well as residents / citizens for various PhilSys services.

b. The SI shall implement a Billing solution supporting the following features.

   1) The proposed billing solution should be flexible so that it can be configured for Business to Business (B2B) and other types of Business to Customer (B2C) services (e.g. paid reprint, paid online update, etc.) in future.

   2) The requirements for the components of the proposed billing solution are as follows:

7.4.16.2.1 Customer Profile Management

a. Manage profiles for different types of TSPs and RPs for the purpose of billing – including authentication request entities such as Authentication / eKYC Relying Parties, profile information including name & address details, email ID, mobile numbers of key contact person(s), agreement details in case of entities, etc.

b. Customer profiles, for authentication request entities, shall be linked to the workflow for on-boarding, issuance of license / API key and invoicing for onboarding.

c. Customer profiles shall be linked to invoices generated, collections made and outstanding receivables, with a facility for online payment through the payment gateway.

d. Detailed Records of customers shall be accessible to PSA and the respective customers through a portal.

e. Allow termination of appointment, for customers such as authentication request entities, due to outstanding receivables, beyond a configurable limit.

f. Customer profiles shall be linked to the online interfaces of CRMS / Contact Center for generation and tracking of service requests.

7.4.16.2.2 Metering & Pricing Configurations

a. This module shall be integrated with the Authentication and eKYC API Gateways for metering of transaction volumes by TSPs and RPs.

b. Support definition of different types of metering configurations in PhP, including uniform pricing, slab pricing, subsidized pricing for specific customers, premium pricing for specific customers, other types of differential pricing (time-based, service-based), pricing for packaging & bundling, etc. including periods of validity.

c. Metering shall also be configurable for specific type of response from the service, e.g. for specific authentication responses and for specific error codes based on each authentication response.

d. Compute price per service transaction e.g. for each authentication, compute the price using the defined metering configurations, authentication response and specific error codes based on the authentication response.

7.4.16.2.3 Invoicing and Receivables management

a. Define and configure standards-based workflow for billing cycle;

b. Generate invoices for customers by triggering the workflow for billing cycle and notify customers;

c. Allow tracking of customer receivables by PSA and allow customers to monitor their accounts, outstanding bills on the PhilSys Web Portal.

7.4.16.2.4 Collections and reporting

a. Configure integration with payment gateway and merchant bank to support all types of payments, generation of payment receipts and recording the corresponding collections in the customer account.

b. Record collections from customers through multiple online payment channels

c. Provide detailed reporting of invoicing status, collections and accounts receivables.

d. Enable tracking failed payments and processing of refunds through the workflow.

7.4.16.3 Other Requirements

a. Integration with Notification System – configure integration with SMS gateway and Email gateway, with configurable templates for SMS and Email notifications; this should be flexible to support other broadcast channels in future.

b. Reporting – provide standard & configurable financial reports for invoicing, receivables, collections, financial accounting;

c. The SI shall conduct detailed requirements gathering, develop detailed design, deployment architecture, provide software development, and support teams for implementing the payment and billing solution.

7.4.17 PhilSys Mobile Application (PMA)

a. The SI MUST design, develop, test, release on main application stores and maintain the PhilSys Mobile Application (PMA).

b. The PMA MUST support all functions described in Section 6.4.1.3 including:

   1) Display static content (images and texts). **The SI MUST include a content management system that can be used by PSA to add, edit or delete all static content visible to the public on the PhilSys Mobile Application.**

   2) Authentication locking / unlocking,

   3) OTP generation,

   4) Management of Alyas PSNs (create, edit, revoke, display under the form of a QR code).

c. The PMA MUST be available for download from Google Play Store and Apple App Store. For example, the SI should always support the app on version N and N-1 of the platforms (where N is the latest version of the Android/IOS at any given point of time)

7.4.18 PhilSys Web Portal (PWP)

a. The SI MUST design, develop, test, install and maintain the PhilSys Web Portal (PWP).

b. The Pre-Registration application MUST be developed as a web application. The SI is expected to launch the pre-registration portal prior to the commencement of the registration.

c. The other functions available on the PWP MUST require the user to authenticate himself/herself using at least OTP via SMS.

d. The SI MUST integrate the Pre-Registration application with PSA website (http://psa.gov.ph/) and all required inputs provided by PSA.

e. The SI MUST ensure that all web pages generated by the PWP web servers will be displayed properly in all major web browsers (HTML 5 / CSS). Web pages and functionality published by the portal must support each of the most common browsers including as a minimum: Chrome, Firefox, Safari. Support for these browsers must include the latest stable version and the version immediately before that.

f. The SI MUST include a content management system into the PWP that can be used by authorized and trained PSA operators in order to add, edit or delete static content visible to the public.

g. The PhilSys Web Portal must be available twenty-four (24) hours every single day and must be secured against sophisticated threats and attacks.

7.4.18.1 PhilSys Web Portal and Mobile Application

The PhilSys Web Portal and PhilSys Mobile App would be used to access the PhilSys Information System for all online transactions and retrieval of information, be it Content Management Components, Customer Relationship Management Application, Partner Management Application, Registration Software Management Application, Quality Check and Manual Adjudication / Verification Application, Pre- Registration, PSN Status Tracking, Public and Private BI Reports/Dashboards views. Residents shall have access to the PhilSys Web Portal. PSA internal users (including partners) shall have separate access to the PhilSys Web Portal.

7.4.18.2 Key Functionalities of the PhilSys Web Portal and Mobile App

The key functionalities of the application are provided below:

a. **Interface to Partner & User Management and Partner Services Overview:** PhilSys Web Portal would contain catalogue for the various available partner services, including details of processes to register /on-board TSPs, required documentation, fees, if applicable, etc.

b. **Resident Services (Pre-Registration, PSN status, PSN Letter Download, etc.):** Resident PhilSys Web Portal/Mobile App would enable residents to check status of their PSN under processing, to download a PSN number digital card , to submit grievance and check its status, update of certain demographic information such as mobile number.

c. **Public and Internal Dashboards:** The resident web portal would show dashboard from the perspectives of registration and identity services. These dashboards will have drill down facility to provide more details to the user, whenever necessary. The internal dashboard will be more comprehensive and may contain the performance measures against predefined KPIs published on a periodic basis in the Business Intelligence and Analytics application. The private dashboards will be accessible by login using Single Sign-On (SSO) feature.

d. **Legal and Governance Framework:** The PhilSys Web Portal Static content would have details on the legal and governance framework.

e. **Resources and Public Relations:** The PhilSys Web Portal would have complete information on the resources and public relations.

f. **Grievance Management:** The internal PhilSys Web Portal would allow the CRMS user to login to the CRMS application using Single Sign-On and perform all call center and grievance redressal activities. Residents would be given an interface where they would be able to file complaints online.

g. **Events, Notices and Circulars:** Portals would contain relevant public notices, events and circulars for viewing.

h. **Other Application Interfaces:** The internal portal would allow the application users to login into respective user applications as per their roles and credentials. For example, adjudication users would login to the adjudication application using Single Sign-On and perform all quality check activities

7.4.18.3 Key Technical Features of the PhilSys Web Portal and PhilSys Mobile App

The overview of the technical solution is given below:

a. Only Internal Portal would be Single Sign-On based portal with single place for different types of users to login using their PSN number along with a second factor of authentication.

b. Information on resident portal would be readable by anyone (public notices, circulars etc.) or using Transaction reference number for tracking PSN application status or using PSN number along with OTP authentication for download of PSN letter.

c. A role-based access would be available to all the users and depending on the role, the user would be able to view and access the applications available for his role on the internal portal.

d. API’s from different applications would be available for consumption by the web portals / mobile app.

e. API's available on Mobile Apps would be exposed using the API Gateway.

f. Portal Access for internal applications like CRMS, Partner Management would be only available on secure lines such Secure internet, MPLS or Secured Network lines etc.

g. Resident Portal would contain link to pre- registration application, status tracking capability for PSN application, download of PSN letter, update of certain demographic features, etc. The resident portal would be available on the internet.

h. All portals would support multilingual features.

i. Software Development Strategy – OTS on Open Source Platform

A depiction of the Portal and Mobile App Components is displayed below.

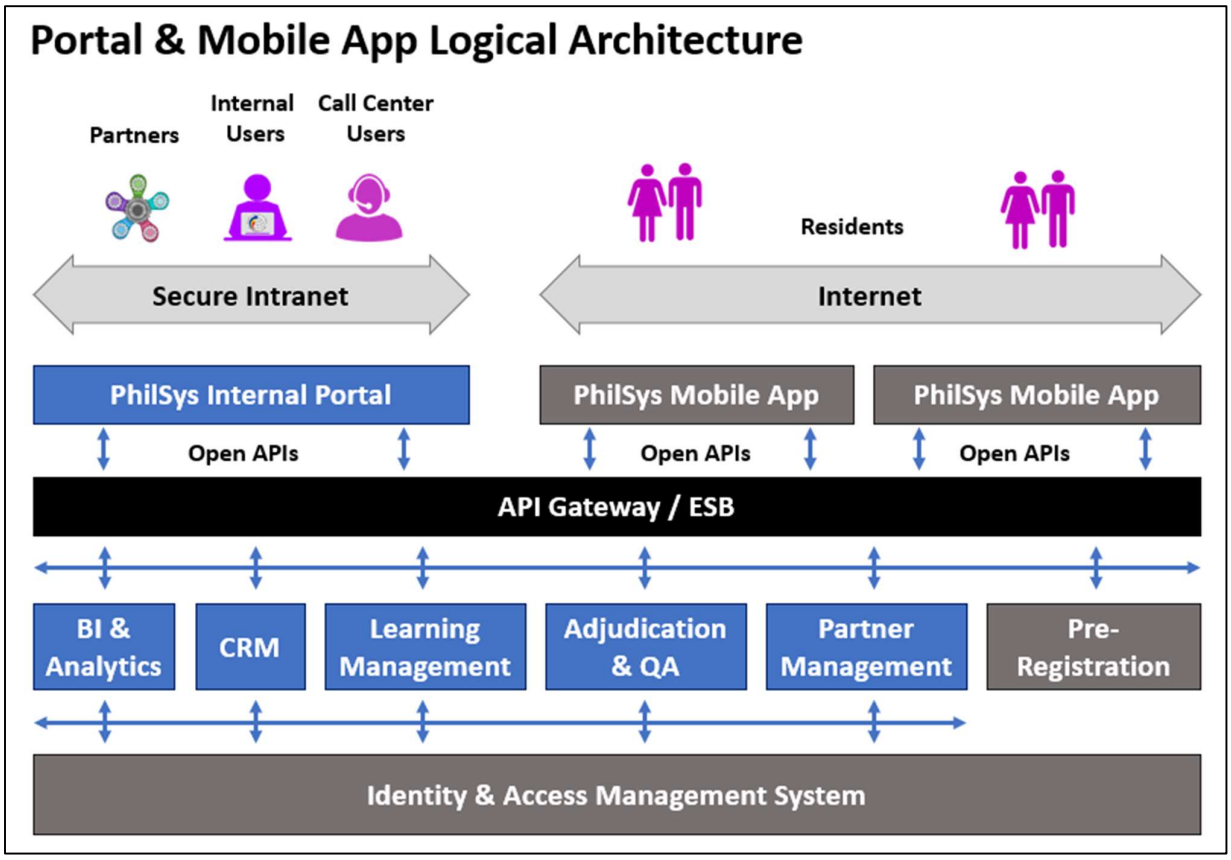

Figure 14. Indicative Portal Architecture

7.5 PhilSys Registry Backup Solution

This section details out the backup and replication guidelines, methods and policies required to be implemented for taking the backup of both type of data stores, i.e. Relational Database Management System and Distributed File System on a regular basis to ensure minimum data loss, effective data recovery and optimum storage requirement.

7.5.1 Key Guidelines for design

a. The section details the key guidelines to be followed for design of Data Store replication solution. Key guidelines cover, Support for Native Database replication solution, Application server/web server configuration synchronization and Automated DR Failover and failback.

   1) Backup solution should have mix of below solutions:

      i. Virtual Backup Media Libraries

      ii. Host and Target Deduplication

      iii. Snapshots backup for OS restoration

      iv. Database Replication

   2) Respective technologies have their own interface, management environment, policy layer, schedulers, recovery processes, and more to orchestrate. This increases management effort of IT staff. It is proposed that respective solution should have common orchestration platform.

   3) Reduced recovery time: Backup software should support heterogeneous backup storage media. In addition, it should also provide middleware (database, SOA, ESB, etc.) specific plugins for backups. This will enable not only faster backup but also faster restoration time. For middleware application, like databases, we can perform point in time recovery, page and table level recovery.

   4) Leverage Deduplication for optimal storage utilization: Deduplication technologies should be leveraged for optimized usage of storage. For databases, target based deduplication should be leveraged and for desktops, host-based deduplication should be leveraged to reduce amount of data getting replicated over network.

b. The key guidelines to be followed for design of Data Center replication solution are given below:

   1) **Support for Native Database replication solution**: DR solutions should support native replication solution provided by databases to ensure databases at both sites are in sync and services can be brought up with minimal downtime.

   2) **Application server/web server configuration synchronization:** Given the large IT landscape for proposed project, it is recommended that configurations post completion of testing should be moved to production and DR simultaneously. Patch level at both the

sites should be same. It is recommended that automated configuration managed tools to be leveraged for application and web servers.

3) **Automated DR Failover and failback:** DR fail-over process should be automated. Post invocation of DR subsequent steps should be automated. Automation involves shutting down of VM's at primary site, stopping of replication at primary site, bringing up of VM's at DR site. On the similar lines, reverse replication activities need to be automated.

7.5.2 Backup Architecture

Backup server will have all the policies configured for file-system backup. In addition, for databases and middleware agent-based backup needs to be configured. Backup solution should support various media types for taking backup. Data will be backed up in disks for a defined duration, as per the backup policy and then data will be moved to backup media for longer storage duration. Deduplication technology is recommended to reduce storage space required for backed up data. Target based de-duplication is recommended for databases and distributed file system. Host based replication is suggested for desktop and file-systems to reduce the amount data which needs to be backed up. VTL will be part of the SAN network. Backup media drives should be placed at different location and in fire and waterproof vault. Backup polices should be configured as per the backup guidelines of respective application.

7.5.3 Replication Solution for Secondary DC

a. For key end user applications like Authentication, EKYC, Portal, PSA wants to ensure zero data loss. As DR is located more than 175 KMs away, in order to achieve zero data loss Secondary DC is required only for critical applications. Secondary DC will be within 50 KMs from Primary Data Center. It should have dedicated dark fiber between DC and Secondary DC with zero hops in between. Round trip latency between primary DC and Secondary DC should be not more than 50 milliseconds.

b. Key applications for which Secondary DC will be leveraged are

   1) EKYC
   2) Authentication
   3) CRMS
   4) Portal
   5) ESM and ITSM DB

c. From secondary DC data will be replicated to DR in asynchronous mode.

d. The location of the secondary DC shall be shared with the Winning Bidder.

7.5.4 Monitoring of Replication and Backup

a. Primary Data Center backup and replication operations needs to be automated and orchestrated as per the backup and replication. Backup activity will be automated as per backup policy. Backup activity monitoring will comprise of following activities:

   1) Number of successful, failed and partial backups
   2) Time elapsed for backup activity
   3) Verifying size of backup
   4) Backup restore status
   5) Backup policy adherence/violations

b. Primary Data Center replication operation monitoring will comprise of following activities:

   1) Replication link bandwidth utilization
   2) Replication success
   3) Replicated data

c. In order to monitor the activities through EMS, integration needs to be done between element monitoring source and correlation engine. Backup and replication monitoring system (can be separate monitoring tool or respective server) can send events and alerts through SNMP, SMTP or ICMP. Correlation engine will perform analysis with other metrics captured by the system.

7.5.5 Replication and Backup Policy

Based on application replication and backup requirement, the replication and backup technology are selected. Synchronous replication can be assessed based on the distance between two data centers and the physical link availability. Asynchronous replication will be followed for non-critical applications.

7.5.6 Requirements of backend replication software

The following table provides the requirements for back-end replication:

Table 45. Requirements of back-end replication software

#	Requirement Description
1.	The proposed Backup Solution should be available on various OS platforms such as Windows and Linux platforms and be capable of supporting SAN based backup / restore from various platforms including Linux, and Windows etc. Backup, replication and SAN solution should be from same OEM

#	Requirement Description
2.	Centralized, web-based administration with a single view of all back up servers within the enterprise. Single console must be able to manage de-duplicated and traditional backups.
3.	The proposed backup solution should allow creating backup clone facility after the backup process.
4.	The proposed Backup Solution has in-built frequency and calendar-based scheduling system.
6.	The proposed backup solution should be capable of taking back up of SAN environment as well as LAN based backup.
7.	The proposed solution also supports advanced Disk staging.
8.	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail for media.
9.	Backup Software is able to rebuild the Backup Database/Catalogue from backup media in the event of catalogue loss/corruption.
10.	The proposed Backup Software should offer online backup for all the Operating Systems i.e. Windows & Linux etc.
11.	The proposed Backup Solution has online backup solution for different type of Databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.
12.	The Proposed backup solution shall provide granularity of single file restore.
13.	The Proposed backup solution shall be designed in such a fashion so that every client / server in a SAN can share Back-Up Database/Library.
14.	Backup Solution shall be able to copy data across firewall.
15.	The backup software should be able to support versioning and should be applicable to individual backed up object's
16.	Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived