महालेखाकार (ले व ह) ,केरल का कार्यालय,
तिरुवनंतपुरम –695001

SUPREME AUDIT INSTITUTION OF INDIA
लोकहितार्थ सत्यनिष्ठा
Dedicated to Truth in Public Interest

OFFICE OF THE ACCOUNTANT GENERAL (A&E)
KERALA, THIRUVANANTHAPURAM-695001

Invitation of Expression of Interest (EoI) for Development of Centralized Correspondence Management System (CCMS)

Contents

Introduction

The Office of the Accountant General (A&E), Kerala, is an integral part of the Indian Audit and Accounts Department, functioning under the Office of the Comptroller and Auditor General of India (C&AG). With its main office located in Thiruvananthapuram and branch offices at Thrissur, Ernakulam, Kozhikode, and Kottayam, the office oversees key accounting and entitlement functions for the Government of Kerala through five specialized wings: Accounts, Pension, GPF, Administration, and Gazetted Entitlement.

This office proposes implementing a **Centralized Correspondence Management System (CCMS)** to serve as a unified digital platform for handling all categories of official communication. The system will cover both **physical and electronic correspondence**, ensuring a structured process for registration, processing, monitoring, and archival of communications. The CCMS will be designed as a **multi-layered solution**, providing modules for:

- Online application management (integration with functional applications such as GPF, GEMS, P-SAI, VLC).
- Offline application management (scanning, OCR-enabled digitization, and workflow routing).
- General correspondence and file workflows (e-files, digital approvals, and dispatch).
- Real-time dashboards, MIS reporting, notifications, and alerts.
- Secure storage, retrieval, audit trails, and integration with external platforms like the *Kerala State Employee Management Portal (KSEMP)*.

The objective is to establish an **end-to-end correspondence management framework** that supports paperless workflows, enables faster decision-making, and provides centralized visibility across the Main Office at Thiruvananthapuram and Branch Offices at Ernakulam, Thrissur, and Kottayam.

Through this Expression of Interest (EoI), the Office seeks responses from **eligible and experienced firms** capable of undertaking the **design, development, implementation, and maintenance** of the CCMS in line with the requirements defined in the ***User Requirement Specification (URS)* document**

2.Scope

The project involves the development and implementation of a **Centralized Correspondence Management System (CCMS)** that will serve as a unified digital platform for handling all official communications across the Main Office at Thiruvananthapuram and the Branch Offices at Ernakulam, Thrissur, and Kottayam. The scope of work to be undertaken by the selected firm is detailed under the following subsections:

2.1 Functional Scope

The CCMS shall cover the complete lifecycle of correspondence, from receipt and registration to routing, processing, approval, and final dispatch. This will include the digital registration of all categories of communication, encompassing online applications, physical submissions, and email-based correspondence. The system shall enable tracking of electronic as well as physical dispatch of responses.

2.2 Digitization and Workflow Automation

The system shall support the digitization of physical documents through integrated scanning and OCR-enabled data capture. This will ensure that offline applications and letters are seamlessly brought into the digital workflow environment. The CCMS will facilitate a paperless office framework by automating the routing of files and communications in line with organizational hierarchies and defined workflows.

2.3 Integration Scope

The CCMS must be capable of integrating with the functional applications presently used in the Office, such as the GPF Module, GEMS, P-SAI, and VLC. This integration shall enable bi-directional flow of data and real-time status synchronization, ensuring continuity of processing between correspondence and domain-specific systems. Additionally, the CCMS should be designed to interface with external platforms like the Kerala State Employee Management Portal (KSEMP), thereby enabling applicants and stakeholders to track the progress of their applications online.

2.4 Monitoring and Reporting

The system shall include a comprehensive Management Information System (MIS) and dashboards for supervisory and administrative use. These features will allow real-time monitoring of pendency, turnaround times, section-wise communication loads, and authorization timelines. The CCMS will also generate periodic and customized reports to facilitate decision-making, compliance verification, and performance reviews.

2.5 Security, Audit, and Data Management

The CCMS shall incorporate robust mechanisms for data security, access control, and audit trails. Role-based access shall be enforced, and all user actions must be logged to ensure accountability and transparency. The system shall provide secure storage and retrieval of documents, regular data backups, and disaster recovery provisions to safeguard against data loss or unauthorized access.

2.6 Deployment, Training, and Support

The scope of work includes end-to-end deployment of the system across the Main and Branch Offices. The selected firm will be responsible for conducting user training programs, preparing comprehensive user manuals and administrative guides, and providing handholding support during the rollout phase. Post-implementation support, maintenance, and system upgrades will also form part of the engagement to ensure the long-term sustainability and scalability of the CCMS.

3. Deliverables

The selected firm shall be required to deliver a fully functional **Centralized Correspondence Management System (CCMS)** in accordance with the requirements specified in the User Requirement Specification (URS) document. The deliverables under the project shall include the following:

3.1 Software Solution

A fully developed and deployed CCMS covering all functional modules, workflows, and integrations as defined in the scope of work. The solution must be secure, scalable, and capable of handling the requirements of the Main Office and Branch Offices.

3.2 System Integration

Seamless integration of the CCMS with existing functional applications such as the GPF Module, GEMS, P-SAI, and VLC, along with linkage to external platforms like the Kerala State Employee Management Portal (KSEMP). The integrations shall be tested and demonstrated to ensure bi-directional data flow and real-time synchronization..

3.3 User Training and Capacity Building

Comprehensive training programs for end-users, administrators, and supervisory officials to ensure effective adoption of the CCMS. Training material, user manuals, and administrative guides shall also be provided in both digital and print formats.

3.4 Documentation

Detailed technical and functional documentation including system architecture, configuration details, integration protocols, data flow diagrams, and security guidelines. End-user manuals and troubleshooting guides shall be part of the deliverables.

3.5 Pilot and Final Deployment

Implementation of the system in a pilot environment for testing and validation, followed by full-scale deployment across the Main Office and all Branch Offices. Issues identified during pilot rollout shall be addressed prior to full deployment.

3.6 Post-Implementation Support

Provision of on-site and remote support for a defined period post-deployment to ensure smooth operation of the system. This shall include bug fixing, performance optimization, and assistance to users during the stabilization phase.

4. Eligibility Criteria

Firms intending to participate in this Expression of Interest must meet the following minimum eligibility criteria:

4.1 Experience

The firm should have at least **three years of experience** in the design, development, and implementation of enterprise-level software solutions. Prior experience in developing **workflow/document management systems** for Government departments, Public Sector Undertakings (PSUs), or large organizations will be given preference.

4.2 Relevant Projects

The firm must have successfully executed at least **two projects of similar nature and complexity**, preferably involving correspondence management systems, workflow automation, or enterprise-wide integration platforms. Documentary evidence, such as work orders or completion certificates, shall be furnished.

4.3 Technical Expertise

The firm should possess adequate in-house technical expertise in software development, system integration, database management, digitization technologies (including OCR), and information security. The availability of qualified professionals such as system architects, software developers, and database administrators must be demonstrated.

4.4 Financial Stability

The firm must have a minimum average annual turnover of **₹1 crore** during the last three financial years. Audited financial statements shall be provided as proof of financial capacity.

4.5 Compliance Requirements

The firm must have valid registration under applicable laws, including Company Registration, PAN, and GST. It should not be currently blacklisted or debarred by any Government department, PSU, or autonomous body. A self-declaration to this effect must be submitted.

4.6 Certifications (Preferred, not Mandatory)

Possession of quality certifications such as **CMMi Level 3 or above, ISO 9001 for Quality Management, and ISO 27001 for Information Security** will be considered an added advantage.

5. Submission Requirements

Firms responding to this Expression of Interest are required to submit the following documents and information as part of their proposal. Each submission must be duly signed and stamped by the authorized signatory of the firm.

5.1 Covering Letter

The submission should begin with a covering letter prepared on the firm’s official letterhead and signed by an authorized representative. The letter must clearly express the firm’s interest in undertaking the project, confirm compliance with the eligibility criteria, and provide an undertaking to furnish additional details if required at later stages.

5.2 Company Profile

A brief but comprehensive profile of the firm is to be included, giving details such as the year of incorporation, legal status, ownership structure, and registered as well as branch office locations. The organizational structure should be outlined, and information regarding the management team and key personnel provided to demonstrate organizational capacity and governance strength.

5.3 Relevant Experience

The firm should provide details of projects executed during the last five years that are relevant to this requirement, especially those involving workflow automation, correspondence management, document management, or enterprise-level system integration. For each project, the client’s name, the scope of work, the project duration, and the overall value should be mentioned, along with the current status of the project. Wherever possible, client references and completion certificates should be furnished.

5.4 Technical Capability

Details of the firm’s technical resources must be presented to establish competence in executing the project. This should include information on the availability of system architects, software developers, database administrators, and cybersecurity experts. Short profiles of the professionals proposed for deployment in this project, highlighting their qualifications and relevant experience, may also be included.

5.5 Financial Details

The firm is required to submit audited financial statements for the last three financial years, along with a summary of turnover figures. This information should demonstrate the financial stability of the firm and establish its ability to sustain the implementation and maintenance of the project. Proof of compliance with the minimum turnover requirements specified in the eligibility criteria must also be provided.

5.6 Certifications and Accreditations

Information on certifications held by the firm, such as CMMi, ISO 9001, ISO 27001, or any other relevant industry standards, should be included. Copies of the certifications must be attached as part of the submission. While not mandatory, such certifications will be considered as an added advantage during the evaluation process.

5.7 Compliance Declarations

The firm must provide a signed declaration confirming that it has not been blacklisted or debarred by any Government department, PSU, or autonomous body. Valid copies of statutory registrations, including PAN, GST, and other applicable registrations, must be enclosed along with the declaration.

5.8 Proposed Approach and Methodology

An indicative note describing the firm’s understanding of the project and its proposed approach to implementation should be included. This note should not exceed five pages and must outline how the firm intends to handle system development, integration with functional applications, deployment, user training, and post-implementation support.

5.9 Indicative Implementation Plan

Firms may provide a high-level outline of the implementation strategy and tentative timelines for the various phases of the project, such as design, development, pilot rollout, full deployment, training, and support. This plan should reflect the firm’s understanding of the project complexity and its ability to deliver within a reasonable timeframe.

5.10 Costing Approach

While detailed financial quotes are not required at this stage, firms may briefly describe their costing approach, such as one-time development charges, license or subscription models, annual maintenance contracts, and support costs. This will only be considered for understanding the financial structure and shall not form the basis of evaluation at the EoI stage.

6. Evaluation Process

The evaluation of the Expressions of Interest will be carried out in a structured manner to ensure fairness, transparency, and objectivity. The process will consist of multiple stages, as outlined below:

6.1 Preliminary Screening

All submissions will first undergo a preliminary screening to verify compliance with the basic requirements of the EoI. This will include checking whether the proposal has been submitted within the stipulated timeline, ensuring that it is duly signed and stamped by an authorized signatory, and confirming the presence of all mandatory documents such as the covering letter, company profile, financial statements, and compliance declarations. Proposals that fail to meet these basic submission requirements may be rejected at this stage.

6.2 Eligibility Assessment

Submissions that pass the preliminary screening will then be evaluated against the eligibility criteria. This assessment will focus on the firm's experience, past performance, technical expertise, financial stability, and compliance with statutory requirements. Only firms meeting the minimum eligibility standards will be considered for the next stage of evaluation.

6.3 Technical Evaluation

Eligible firms will be assessed on the basis of the information provided in their submissions, particularly their relevant project experience, technical capabilities, certifications, and indicative approach and methodology. The evaluation will also take into account the firm's proposed implementation plan and its ability to provide sustainable post-implementation support. Firms demonstrating proven expertise in developing and implementing workflow/document management systems and integration with multiple applications will be rated more favorably.

6.4 Presentations and Clarifications

Shortlisted firms may be invited to make a presentation before the Evaluation Committee. The purpose of the presentation will be to assess the firm's understanding of the project, proposed solution approach, and capacity to deliver. During this stage, the Committee may also seek clarification on the information submitted in the EoI.

6.5 Shortlisting for RFP

Based on the outcome of the technical evaluation and presentations, a final list of shortlisted firms will be prepared. These firms will be formally invited to participate in the next stage of the process, which will be the issuance of the Request for Proposal (RFP). The RFP will include detailed functional and technical requirements, along with instructions for submission of financial proposals.

7. Important Dates

The following timeline shall be adhered to for this Expression of Interest process. Any changes to these dates will be notified on the official website of the Office of the Accountant General (A&E), Kerala, or communicated directly to the firms concerned as appropriate

Activity	Date & Time	Remarks
Issue of EoI Document	07.10.2025	Published on official website / notice board
Last Date for Submission of Queries/Clarifications	15.10.2025	Queries to be submitted via email to the designated officer
Clarifications to be Published	21.10.2025	Responses will be shared with all interested firms
Last Date & Time for Submission of EoI	31.10.2025	Submissions to be made at the address/email provided in Section 10
Opening of EoI Submissions	04.11.2025	In the presence of authorized representatives of firms, if required
Completion of Evaluation Process	10.11.2025	Indicative timeline, subject to change
Notification of Shortlisted Firms	15.11.2025	Shortlisted firms will be invited to the RFP stage subject to the decision of Competent Authority.

.

8. Contact Information

For further details and clarifications please contact:

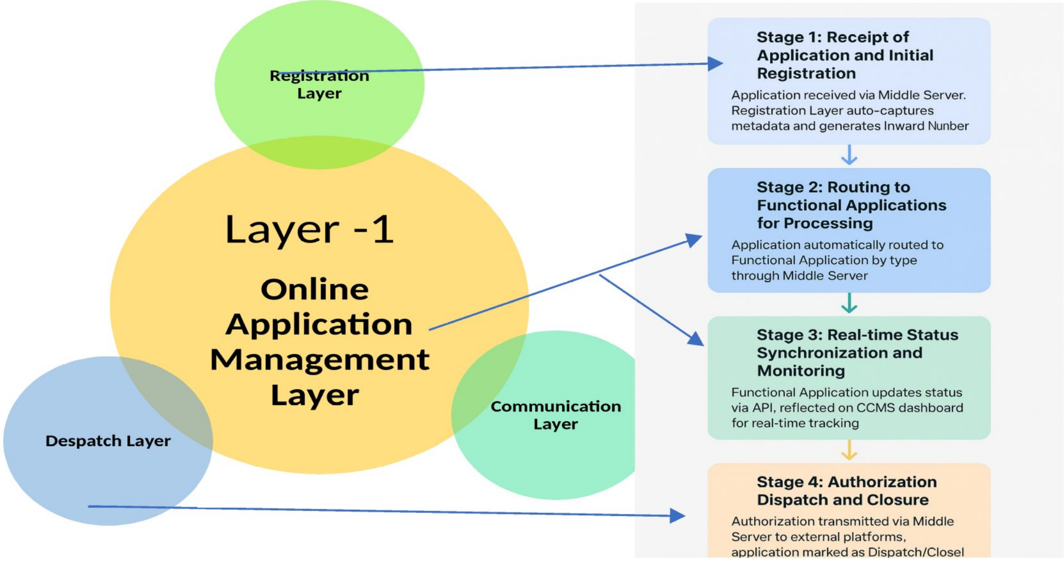
Name: Yogesh A, Sr. Accounts Officer / ITS
Email: agaekerala@cag.gov.in, yogesha.ker.ae@cag.gov.in, dmitscell.ker.ae@cag.gov.in
Phone: 9447388343, 8157044693

Senior Accounts Officer / ITS Cell

Annexure I Functional Requirements.

CCMS Layer -1-Functionalities

The Online Application Management Module is the first and most critical layer of the CCMS architecture. It is designed to handle all entitlement-related online applications that are received electronically through Middle Server Solutions and processed through various functional applications such as GEMS, GPF Module, P-SAI, and VLC. This module ensures the seamless integration, tracking, and end-to-end status management of online applications from receipt to final authorization and dispatch.



Stage 1: Receipt of Application and Initial Registration

Application received via Middle Server. Registration Layer auto-captures metadata and generates Inward Nunber

Stage 2: Routing to Functional Applications for Processing

Application automatically routed to Functional Application by type through Middle Server

Stage 3: Real-time Status Synchronization and Monitoring

Functional Application updates status via API, reflected on CCMS dashboard for real-time tracking

Stage 4: Authorization Dispatch and Closure

Authorization transmitted via Middle Server to external platforms, application marked as Dispatch/Closel

A. Sub-Layers and Functional Scope

1. Registration Sub-Layer

The Registration Sub-Layer serves as the intake gateway for all online applications. It interfaces directly with the Middle Server and performs the following functions:

- **Auto-Capture of Application Metadata:** On receipt of a new application via the Middle Server, the system extracts metadata including Acknowledgement Number, PEN, Application Type, and Date of Receipt.
- **Generation of Unique Inward Number:** Each application is assigned a unique inward number in CCMS, mapped to the Acknowledgement Number generated by the Middle Server.
- **Mapping to Functional Applications:** Applications are tagged and routed to the respective functional modules through middle servers (e.g., GPF, Pension, GE) based on the application type.

- **Timestamping and Reference Logging:** All registrations are timestamped, and logs are maintained for audit and compliance tracking.

2. Communication Sub-Layer

The Communication Sub-Layer ensures real-time connectivity and status synchronization between CCMS and the functional applications.

- **Bidirectional API/Web Service Integration:** Secure APIs connect CCMS with GPF Module, GEMS, Pension SAI, and VLC, enabling continuous status updates.
- **Status Reflection in CCMS:** Each stage of processing—pending, under process, authorized—is reflected in real time in the CCMS dashboard.

3. Despatch Sub Layer

Once the case is processed and authorization is generated, the status is updated automatically through Middle Server confirmation in Despatch Sub Layer

B. End-to-End Workflow Stages

The **Online Application Management Module** in CCMS follows a structured, fully automated workflow, designed to seamlessly track online applications from receipt to authorization and dispatch. The end-to-end process involves four key stages as described below:

Stage 1: Receipt of Application and Initial Registration

At the first point of contact, online applications are received from stakeholders through external service portals (e.g., HRMS, KSEM Portal), which transmit the data into the office environment via Middle Server Solutions. These middle servers act as intermediaries that gather basic application metadata such as the Acknowledgement Number, PEN, Application Type, and Date of Submission**.**

As soon as an application enters the system, the Registration Layer of the CCMS automatically captures this information and generates a unique Inward Number, thereby creating a formal record of receipt. This inward number is then mapped to the Acknowledgement Number received from the Middle Server, ensuring traceability across platforms. This registration step marks the official entry of the communication into the digital workflow, with proper timestamping, section tagging, and linkage to subsequent actions.

Stage 2: Routing to Functional Applications for Processing

Once registration is completed, the application and its associated metadata are routed to the corresponding **Functional Application** based on its type. For example, a GPF Advance application is directed to the **GPF Module**, while a Pension Authorization case is forwarded to **Pension-SAI**. This routing is automated, governed by pre-configured mapping rules within CCMS.

The transmission is performed through the **Middle Server**, which ensures safe delivery of the case file to the functional application without user intervention. At this stage, the application is ready for domain-specific processing—such as scrutiny, validation, and authorization generation—inside the concerned functional software.

Stage 3: Real-time Status Synchronization and Monitoring

As the application undergoes various stages of processing inside the functional application, the current **status is continuously pushed back to CCMS** through a secure **API or Web Service interface**. Each change in the case's state whether it's marked as *Pending*, *Under Process*, *Reverted*, *Authorized*, or *Rejected*—is captured by the **Communication Layer** of CCMS.

These live status updates allow users and supervisory officials to monitor the real-time progress of each application via the CCMS dashboard. The system not only reflects the current stage of disposal but also records **timestamps for each transition**, creating a clear audit trail. This stage ensures **transparency**, reduces the need for manual status enquiries, and significantly improves stakeholder responsiveness.

Stage 4: Authorization Dispatch and Closure

After the case is processed in the functional application and the authorization is generated, the final output (e.g., GPF Sanction Order, Pension Authorization) is transmitted electronically via the Middle Server to the external platforms like KSEM Portal, State HRMS, or Treasury application, depending on the type of case.

The CCMS captures this final dispatch activity in its Dispatch Layer, marking the application as *Dispatched* or *Closed* upon confirmation of successful delivery. The status is updated in both the Communication Layer and Reporting Dashboard, allowing section users and controlling officers to verify that the case has been disposed of correctly.

This stage completes the application's lifecycle in CCMS. All associated documents, status logs, dispatch details, and references remain archived in the system, accessible for future retrieval, reporting, or audit verification.

C. Key Functional Features

Feature	Description
Automated Application Capture	Data fetched directly from Middle Server
Unique Inward Numbering	System-generated number for tracking and logging
Real-time API Synchronization	Live status updates from functional applications
Dispatch Monitoring	CCMS tracks whether e-authorizations are sent to respective external platforms
Dashboard Reporting	Real-time status visibility across all wings and applications
No Manual Intervention	Fully automated process flow from registration to disposal

D. Benefits

The Online Application Management Module (Layer-1) serves as a critical automation layer in the Centralized Correspondence Management System (CCMS), offering significant functional and operational benefits across departments. Its introduction is expected to enhance communication processing efficiency, reduce workload duplication, and strengthen oversight mechanisms. The key benefits are outlined below:

One of the most immediate advantages is the elimination of duplicate data entry and manual tracking. Since application data is captured directly from the Middle Server and passed to functional applications through automated interfaces, the need for clerical staff to manually log, record, or re-enter details at multiple stages is removed. This reduces clerical burden, lowers the risk of human error, and improves data consistency across systems.

The module also enables centralized and real-time monitoring of entitlement workflows. Applications related to pension, GPF, or GE are routed through their respective functional software, but their status at each stage of processing is continuously reflected in the CCMS dashboard. This gives both section users and supervisory officers a unified view of all pending, processed, and dispatched communications, fostering transparency and operational discipline.

By streamlining the application routing process, the system significantly improves turnaround time. Cases that earlier required physical forwarding, tracking through multiple registers, and follow-up calls are now processed through pre-configured digital workflows. This not only expedites movement between layers but also minimizes delays caused by unclear handoffs or lost documentation.

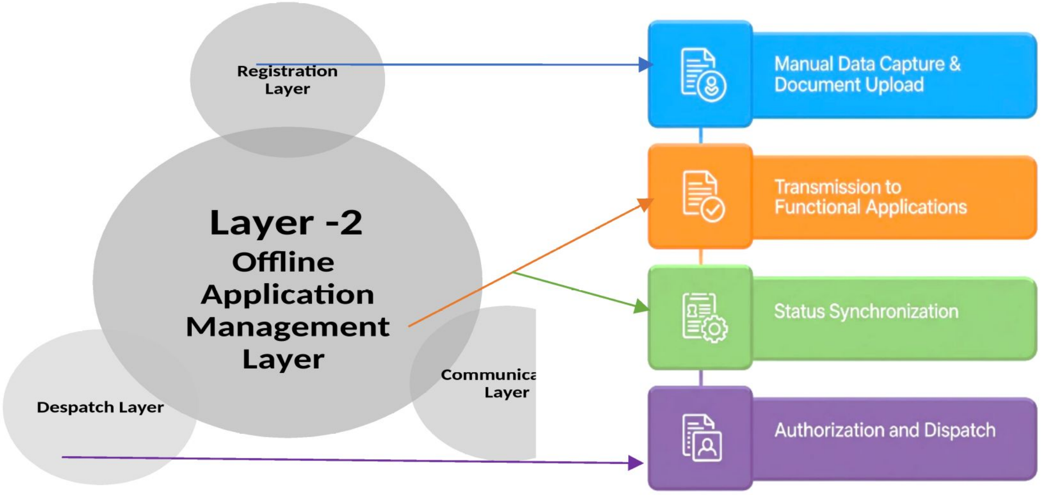
Another major benefit is the availability of audit-ready logs and complete communication metadata for every application. Each stage—registration, routing, processing, and dispatch is timestamped and recorded. This ensures accountability, simplifies internal review, and allows for efficient responses to audit or RTI queries.

Finally, the module ensures seamless synchronization between functional systems and the central communication tracker. By establishing bi-directional connectivity via APIs, CCMS ensures that updates made in domain-specific applications are automatically reflected in the central monitoring system. This eliminates inconsistencies in status reporting and ensures that all stakeholders operate from the same authoritative information base.

B. CCMS Layer -2-Functionalities

The **Offline Application Management Module** constitutes the second core layer of the Centralized Correspondence Management System (CCMS). This module is designed to handle applications that are received in **physical form (post, hand delivery)** or via email channels, which still form a significant portion of application in entitlement processing, especially in categories such as foreign deputation, reissue cases, service verification, and older pension claims.

Layer 2 ensures that such offline applications are brought into the same structured, trackable, and audit-ready workflow as online applications by supporting **manual registration, scanning, workflow-based routing, and status synchronization** with functional applications.


Registration Layer
Layer -2
Offline Application Management Layer
Despatch Layer
Communica
Layer
Manual Data Capture & Document Upload
Transmission to Functional Applications
Status Synchronization
Authorization and Dispatch

A. Sub-Layers and Functional Scope

1. Manual Registration and Data Entry Sub-Layer

This sub-layer facilitates the entry of details for offline applications that are not received via the Middle Server. Key functionalities include:

- **Manual Inward Registration Interface**: Enables authorized users (inward clerks) to enter the basic details of the application—name, PEN, application type, date, sender information, etc.—and generate an inward number.
- **Scanning and Uploading of Documents**: Physical documents received via post or hand are scanned at the point of receipt. Scanned files are uploaded and tagged to the corresponding inward number. The system shall integrate **Optical Character Recognition (OCR)** capabilities within the scanning interface used in the Physical Application Inward Module. This will allow auto-extraction of key data fields such as applicant name, PEN, GPF number, subject, and date from scanned documents. OCR will significantly reduce manual data entry time during registration and improve accuracy. The extracted text shall be pre-populated in the registration form, with the option for manual correction and confirmation by the user.
- **Email Registration Option**: Applications received as attachments through official email inboxes are also registered here, with attached PDFs linked to the respective inward record.

2. Routing and Integration with Functional Applications

This sub-layer ensures offline applications follow the same integrated processing pipeline as online ones:

- **Pushing Metadata and Scanned Files via API/Web Services**: Once an application is registered and scanned, it is forwarded to the appropriate functional application (GEMS, GPF, P-SAI) for processing via middle servers.
- **Change Management in Functional Applications**: Functional software must be updated to accept Offline applications along with the scanned supporting documents and return status updates at each stage of the processing lifecycle to CCMS.

3. Despatch Sub Layer

- Once the case is processed and authorization is generated, the status is updated automatically through Middle Server confirmation in Despatch Sub Layer

B. End-to-End Workflow Stages

Stage 1: Manual Data Capture and Document Upload

Offline applications received via post or hand delivery are first registered in the CCMS through a manual data entry interface. Basic metadata is entered, and the document is scanned using smart scanners (where deployed). The scanned copy is uploaded into the CCMS and tagged to the application's inward number. If the document is received via email, it is diarised and the email attachment is similarly linked.

Stage 2: Transmission to Functional Applications

Upon successful registration, the metadata and uploaded document are sent to the relevant functional application through APIs/Web Services. The functional software must support this intake mechanism and accept the documents for further action—this requires coordination and system-level changes at the functional application side.

Stage 3: Status Synchronization

As the application is processed by the functional wing, its status is periodically updated and returned to the CCMS through the integration interface. This real-time synchronization allows users and supervisors to view the processing status of offline applications in the same dashboard as online ones.

Stage 4: Authorization and Dispatch

Depending on the nature of the case, the final authorization may be issued electronically or physically:

If e-authorization is generated, it is routed through the Middle Server as in online cases.

If the authorization is physical, the document is uploaded into the CCMS and manually dispatched via post or email from the CCMS Dispatch Module.

C. Key Functional Features

Feature	Description
Manual Registration Interface	For data entry of physical or email-based applications
OCR-Based Data Extraction During Registration	This will allow auto-extraction of key data fields at the time of document scanning.
Document Scanning Integration	Scanned files attached to each inward entry
Functional Software API Push	Metadata and documents pushed to GPF, GEMS, P-SAI via secure APIs
Email Diarisation	Built-in support for registering and tagging email-based applications
Real-time Status Tracking	Status updates from functional applications displayed

	on CCMS dashboard
Dispatch Layer Support	**Manages both electronic and physical dispatches** with tracking

D. Benefits

The Offline Application Management Module fills a critical functional gap by introducing structure and visibility into communication processes that originate outside digital channels. Despite the growing adoption of online systems, a substantial volume of applications and requests—such as service verification, pension revisions, or deputation requests—still arrive in physical form or through unstructured emails. This module ensures that these non-digital inputs are not excluded from centralized tracking and processing.

One of the key benefits of this module is that it ensures comprehensive coverage of all communication, regardless of format or origin. Every physical document, handwritten application, or emailed request is formally registered in the CCMS, assigned a unique inward number, and routed into the same monitored workflow as online cases. This significantly improves control, accountability, and departmental coordination, as no application can go unrecorded or unprocessed due to format limitations.

It also establishes a unified process across both online and offline workflows. The same routing logic, processing stages, and dashboard visibility are applied to physical and electronic cases alike. This allows for seamless integration with existing reporting systems, avoiding the need to manually reconcile data from disparate tracking sources. Functional applications such as GPF, GEMS, and P-SAI receive and process both online and offline cases using standardized APIs, which results in uniformity of case management.

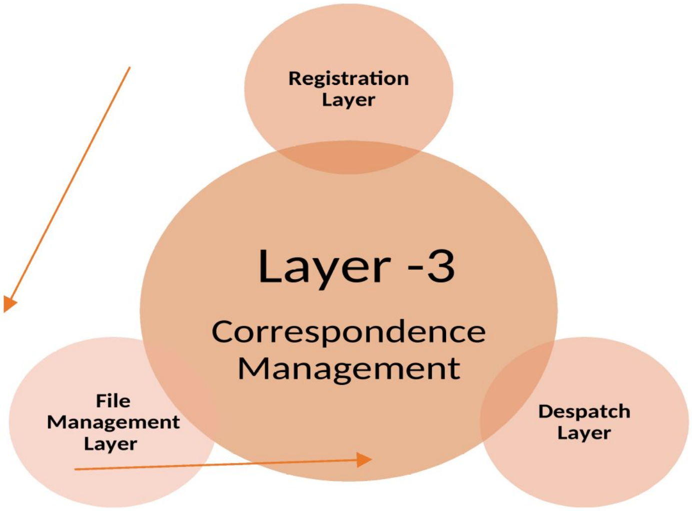
Another major advantage is the reduction of manual dependency. With features like scanning integration, email diarisation, and structured metadata capture, the module digitizes offline communications at the point of entry. Clerical staff no longer need to maintain separate paper registers or track status manually. Scanned documents are uploaded once and move digitally through the processing pipeline, ensuring faster movement and fewer handling errors.

The module also brings offline cases under centralized monitoring. Real-time status updates from functional applications are reflected in the CCMS dashboard, giving supervisors and section heads full visibility into the pendency and movement of all cases, regardless of how they were submitted. This improves oversight and allows for timely intervention where delays are observed.

C. CCMS Layer -3-Functionalities

The Correspondence Management and File Workflow Module forms the third core layer of the Centralized Correspondence Management System (CCMS). This module addresses all types of communications that are not directly linked to functional authorizations but still require responses, internal actions, or documentation. These include communications from HQrs, Government departments, RTI authorities, legal bodies, and internal sections—many of which cannot be mapped to domain-specific applications.

This module brings all such communications into a workflow-driven, paperless environment by offering an integrated digital file management system. It supports the full lifecycle of correspondence handling, from registration and diarisation to file noting, drafting, approval, and dispatch.



A. Sub-Layers and Functional Scope

1.Registration and Diarisation Sub-Layer

This sub-layer handles the intake of communications requiring action or filing, received via post, hand delivery, or email.

- **Manual and Email-Based Registration**: All physical communications are manually registered and scanned and uploaded in the Diarisation Sub - Layer. The system shall integrate **Optical Character Recognition (OCR)** capabilities within the scanning interface used in the Physical Application Inward Module. This will allow auto-extraction of key data fields such as applicant name, PEN, GPF number, subject, and date from scanned documents. OCR will significantly reduce manual data entry time during registration and improve accuracy. The extracted text shall be pre-populated in the registration form, with the option for manual correction and confirmation by the user, while emails received in official mailboxes are auto-fetched through the CCMS mail server and diarised.

- **Metadata Capture and Tagging**: Inward entries include sender details, subject, department, priority level, and communication type, allowing for efficient tracking and routing.
- **Automated Routing to Section Heads**: Registered documents are routed to the respective section head's CCMS inbox, based on pre-configured mapping.

2. File Management Sub-Layer

This is the core of the module and simulates a full digital file management system, similar to e-Office.

- **Electronic File Creation**: Users can create new files or append new receipts to existing digital files.
- **Note and Draft Modules**: Users can prepare notes, create drafts, and link references within the system.
- **File Routing and Action Flow**: Files can be routed for review, approval, or higher-level endorsement. Movement is tracked and timestamped.
- **Digital Signature Support**: Authorized users (e.g., Section Heads, SAOs,DAGs,AG) can apply digital signatures for file approval and communication dispatch.

3. Dispatch Sub-Layer

This sub-layer handles the dispatch of replies or decisions after processing is completed.

- **Email Dispatch Facility**: Drafted replies or signed orders can be sent directly from the system via integrated email dispatch.
- **Physical Dispatch Interface**: If required, documents are handed over to the dispatch section, and manual dispatch details are entered into CCMS.

B. End-to-End Workflow Stages.

Stage 1: Registration and Routing

Communications received by post or hand delivery are registered in the CCMS by the inward Data Entry Operators. Physical copies are scanned and uploaded at the time of registration. Email communications are pulled automatically into the CCMS Mail Server inbox and diarised by the General (Inward) Section. Based on predefined workflows, the document is then forwarded to the inbox of the relevant Section Head.

Stage 2: Assignment and File Creation

Section Heads review incoming communication and assign it to the appropriate Dealing Units. The units either appends it to an existing file or creates a new digital file in the File Management Layer then begins file noting, prepares a draft reply or proposal, and sends the file for review.

Stage 3: Review, Signature, and Finalization

The Section Head or Supervisory Officer reviews the file, adds notes if necessary, and digitally signs the final draft or recommendation. Approved communications are forwarded to the dispatch layer.

Stage 4: Dispatch and Closure

The final response is dispatched either by email (using the CCMS mail server) or physically (entered manually in the dispatch section interface) by the originating unit. Once dispatched, the file and its communication are marked "Closed," and the entire activity is logged for reference.

C. Key Functional Features

Feature	Description
Email Diarisation	Automatic capture and registration of communications received via email- mailbox facility
Manual Registration Interface	For data entry of physical or email-based applications
Document Scanning Integration	Scanned files attached to each inward entry
OCR-Based Data Extraction During Registration	This will allow auto-extraction of key data fields at the time of document scanning
Digital File Creation	Users can initiate or update e-files linked to communications
Internal Note and Drafting Tools	Supports drafting of replies, file movement, and documentation
Workflow Routing Engine	Tracks document movement across officers and sections
Digital Signature Integration	Section Heads and Supervisory Officers can digitally sign files
Audit Trail and Communication Logs	Maintains history of file movements, actions, and dispatch
Email and Physical Dispatch Support	Replies can be sent electronically or physically, with dispatch tracking

D. Benefits

This module introduces a structured, paperless, and accountable environment for handling communications that traditionally operate outside functional systems. It ensures that every type of correspondence whether a departmental query, policy letter, RTI application, or court directive—is managed in a traceable and efficient manner.

By providing a file-based digital workflow, the module allows for quick collaboration between assistants, section heads, and supervisory officers without reliance on physical files. It reduces delays, enables transparency in approvals, and supports compliance documentation. The incorporation of digital signatures and email dispatch reduces the time and cost associated with manual processing, while ensuring authenticity.

Moreover, the centralization of correspondence ensures that communications across all wings—administrative, functional, and supervisory—are processed under a single platform, aligning with the goal of digital transformation and transparent governance.

D. CCMS Reporting and Dashboard-Functionalities

The Reporting and Dashboard Functionalities in the Centralized Correspondence Management System (CCMS) are designed to provide users especially supervisory and administrative officials—with actionable insights, real-time visibility, and comprehensive oversight across all types of communications. These features are critical for monitoring pendency, evaluating performance, ensuring compliance, and supporting informed decision-making at all levels of the organization.

This module aggregates data from all core layers online application management, offline application processing, and correspondence workflows and presents it through customizable dashboards and structured reports. The reporting layer also plays a vital role in responding to audit queries, reviewing section-wise efficiency, and ensuring that service delivery timelines are met.

A. Functional Scope of the Reporting and Dashboard Module

1. Real-time Dashboards

The system shall feature interactive dashboards with graphical summaries of communication status, including charts, tables, and filters for data segmentation.

Key dashboard elements include:

- **Inward Status Overview:** Real-time counts of received, processed, pending, and dispatched communications across all layers.
- **Section-wise Load and Performance:** Displays communication volumes, turnaround times, and pendency per section or branch office**.**
- **Case Ageing Analysis:** Highlights long-pending applications or files, categorized by duration (e.g., 0–7 days, 8–15 days, 15+ days).
- **Dispatch Summary:** Shows data on electronic and manual dispatches completed per section**.**

- **Authorization Timeline Tracker:** For online and offline applications requiring authorization, the dashboard shows processing timelines and identifies delays.

2. MIS Reports

The CCMS will generate standard and ad-hoc Management Information System (MIS) reports in printable and exportable formats (e.g., PDF, Excel).

Types of reports include:

- Daily/Weekly/Monthly Inward and Disposal Report
- Section-wise Pendency Report
- User-wise Activity Report
- Application Type-wise Status Report (e.g., GPF Advance, Pension Authorization)
- Dispatch Register Report
- Offline Application Tracking Report
- Communication without Action/Reply Summary

3. Custom Report Builder

The system shall provide a customizable report generation tool for authorized users to define filters, groupings, and fields (e.g., by date range, section, communication type, or status). This will allow officials to create tailored reports to suit internal reviews, RTI replies, or audit compliance.

B. Key Features

Feature	Description
Live Dashboard	Real-time summary of communication across all layers
Section and User Analysis	Tracks performance and load by section, wing, and user
Aging and Pendency Insights	Flags delayed communications and overdue cases
Configurable Report Builder	Enables creation of custom filters, views, and fields
Export & Email Integration	Reports can be downloaded /printed
Drill-down Navigation	Allows movement from dashboard summaries to individual record details

C. Benefits

This module empowers the organization with a data-driven view of communication workflows, enabling better control, faster decision-making, and improved service delivery. By providing clear visibility into the lifecycle of every communication, it strengthens accountability and transparency.

Supervisory officials can monitor workload trends, quickly intervene in delayed cases, and take data-backed decisions.

E. E-File Functionality (Stakeholder-Centric Document View)

The Centralized Correspondence Management System (CCMS) shall include a comprehensive E-File module that enables a unified, stakeholder-centric view of all communications, applications, and documents processed across various wings of the office. Since different wings handle different categories of work and use diverse metadata formats—such as PEN in GPF-related cases, PPO number in pension processing, or GE number in pay entitlement—the system shall maintain a cross-referenced metadata structure that connects all identifiers to a single stakeholder profile. This will allow authorized users to view the entire history of communications related to a stakeholder, irrespective of the section through which it was received or processed.

The E-File interface will provide powerful search, filter, and sorting functionalities, allowing users to retrieve documents based on stakeholder name, PEN, GPF account number, PPO number, GE number, receipt number, date of receipt, type of receipt (e.g., GPF, NRA, Pay Fixation), or status (e.g., pending, under process, cleared, returned). All such documents—including scanned inward communications, file notes, draft replies, final approvals, and dispatch copies—shall be accessible from the stakeholder’s E-File panel. Users can view, download, or forward these documents as per their access privileges.

This functionality will be especially useful in entitlement processing, audits, and RTI handling, where a complete and chronological view of a stakeholder's history is essential. The system shall allow section-wise and time-based sorting of documents, enabling efficient analysis and reference. Role-based access control will ensure that dealing units view only those stakeholder files relevant to their assigned sections, while section heads and supervisory officers may access all transactions across multiple wings. The E-File thus supports end-to-end visibility, reduces redundancy, and improves coordination between sections, contributing significantly to the office’s goal of creating an integrated, paperless, and stakeholder-focused environment.

F. Search and Filtering Capabilities

The Search and Filtering Capabilities within the Centralized Correspondence Management System (CCMS) form a vital cross-cutting feature that supports efficient information retrieval, document traceability, and real-time access to communication records. This module enables users—across all roles and privileges—to retrieve registered communications, files, and related actions using intuitive search interfaces and dynamic filters. These capabilities contribute significantly to operational productivity, response readiness, audit compliance, and supervisory oversight.

A. Functional Scope of Search and Filtering

The search and filtering functionalities of the CCMS are designed to facilitate fast, intuitive, and reliable access to all communication records within the system. A centralized search interface, accessible from the main dashboard and across all modules, allows users to retrieve information using a wide range of input fields. These include inward number, acknowledgment number, PEN, file number, name, sender, department, application type, subject, or date of receipt. Users can search even with partial entries or keywords, and the system dynamically fetches the most relevant results.

To refine search results further, the CCMS offers advanced, multi-layer filtering options. Users can apply filters based on section or branch office, communication category (such as online applications, offline entries, or correspondence), processing status (received, under process, dispatched, closed), priority level, mode of receipt (physical, email, or portal-based), and date ranges. This ensures that even in a high-volume environment, records can be located with precision and minimal delay.

One of the most significant capabilities of this module is its support for cross-module search. A single query, such as a PEN number or subject keyword, can fetch results from online application records, offline entries, and the file workflow module, enabling a consolidated view of all communication linked to a particular person or subject. This interconnectivity ensures comprehensive traceability and reduces the need to consult multiple systems.

The system also allows users to save frequently used search combinations as custom presets, facilitating repeat queries with a single click. The search results are presented in a clear tabular view, displaying key metadata such as inward number, subject, current status, last action, and assigned section. From this screen, users can directly open communication records, forward items, download documents, or export the list to Excel or PDF. This design ensures that the search module serves not just as a retrieval tool but as a gateway to further action.

B. Key Features

Feature	Description
Global Search Bar	Keyword-based search across all modules
Advanced Filters	Multi-criteria filtering for precise data extraction
Module-Wide Coverage	Searches span online applications, offline entries, correspondence, files

Saved Search Profiles	Frequently used filters can be saved and reused
Exportable Search Results	Results can be printed or exported to common formats
Search-Linked Actions	Users can view, open, forward, annotate, or print records directly from search view on the basis of their access roles

G. Notification and Alerts

The Notification and Alerts Module in the Centralized Correspondence Management System (CCMS) is designed to deliver timely and targeted communication to both internal users (clerks, assistants, officers, administrators) and external stakeholders (applicants and correspondents), based on the status and progress of communications or applications. The module ensures that every actor in the communication lifecycle is kept informed through system-generated alerts, reminders, and status updates—minimizing delays, improving accountability, and supporting end-to-end transparency.

This module supports multiple notification levels, customized per user role and communication type, and is integrated with email servers and SMS gateways to facilitate multi-channel delivery.

Functional Scope of Notifications and Alerts

1. Internal Task-Based Alerts

The system generates real-time alerts for internal users whenever:

- A new communication or file is routed to the user's inbox.
- A document requires drafting, review, or approval.
- A case is returned for revision, resubmission, or clarification.
- An authorization is pending dispatch.
- Communication remains unprocessed beyond a defined threshold (e.g., 5 or 10 working days).

These alerts are visible within the user's dashboard and can optionally be sent via email or popup notifications to ensure timely attention.

2. Stakeholder Notifications.

In addition to internal alerts, CCMS will support **direct communication with applicants and external stakeholders** whose cases are being processed.

- **Email Notifications to Applicants**: At every key stage (e.g., Registration, Under Process, Authorized, Dispatched), the system shall trigger status update emails to the stakeholder's registered email address, providing reference numbers, current status, and any additional instructions or outcomes.

- **SMS Alerts (Optional / Phase-wise Implementation)**: For critical updates such as application receipt, authorization completion, or dispatch a brief status message may be sent to the applicant's registered mobile number via SMS gateway integration. This ensures reach even in low-connectivity or non-digital environments.
- **Communication Templates**: Messages sent to stakeholders will follow standardized formats approved by the department, including unique identifiers like Inward Number, Acknowledgement Number, and expected turnaround actions (if applicable).

This functionality shall be tightly integrated with the CCMS–KSEM Portal interface, ensuring **real-time reflection of updates** for applicant visibility

H. Integration with other Systems

The Centralized Correspondence Management System (CCMS) is designed as a unified communication backbone that not only manages registration, routing, tracking, and dispatch of communications but also functions as a central integrator across internal functional applications and external platforms. The system shall support bidirectional integration with the office's domain-specific software applications, middleware services, and external stakeholder-facing portals like KSEM Portal, ensuring seamless data flow and real-time status synchronization.

This section outlines the multi-level integration strategy that CCMS will adopt to ensure interoperability, traceability, and service delivery continuity.

A. Integration with Internal Functional Applications

As described in the online application and offline application management layer, the CCMS integration proposed with the following internal applications

- GEMS (Gazetted Entitlement Management System) **– DB – Oracle 11g, Application - Java**
- GPF Module – DB **& Application in Oracle 11g**
- P-SAI **– DB& Application in Oracle 12 C**
- VLC (Voucher Level Computerisation) **– DB & Application in Oracle 11g**

This integration shall follow an architecture, allowing CCMS to communicate with systems operating on different platforms or developed using different technologies through APIs / Webservices. Status synchronization from functional applications will be reflected in the CCMS dashboard, ensuring full traceability for supervisory users.

B. Integration with Middle Server Solutions.

The CCMS needs to integrate with the various middle server applications which serve as intermediaries between the external application portals and internal processing systems for status updates and sharing the offline applications with the functional applications (detailed in **3.4 CCMS Layer -2-Functionalities)**

C. Integration with Kerala State Employee Management Portal (KSEMP)

The Centralized Correspondence Management System (CCMS) is envisioned to function not only as an internal tracking and processing system but also as a **communication bridge between the office and external platforms**, particularly the **KSEM Portal**—which acts as the front-end interface for stakeholders such as government employees and pensioners for accessing entitlement-related authorizations.

To ensure seamless stakeholder experience and transparency in service delivery, the CCMS shall be **integrated with the KSEM Portal through a secure, real-time API/Web Service framework**. This integration will allow the data captured, processed, and finalized within CCMS to be transmitted automatically to the KSEM Portal, enabling applicants to track the progress of their requests without manual follow-up or intervention.

The integration will ensure that, once an application is registered and mapped in CCMS—whether it originates as an online application through the Middle Server or as a physical/offline submission—its processing status will be updated in real time to the KSEM Portal at every critical stage: registration, processing, authorization, and dispatch. Each update made in CCMS (such as “Received,” “Under Process,” “Reverted,” “Authorized,” or “Dispatched”) will be automatically reflected in the applicant’s view on the portal.

In summary, the CCMS–KSEM Portal integration will enable:

- Real-time status synchronization of applications between the internal CCMS and KSEM portal.

- Transparent service delivery by allowing applicants to track their communication or application status at any stage.
- Reduction in manual query handling, freeing up staff time and ensuring faster, applicant-driven status access.
- Enhanced accountability, as the timestamps and processing trail maintained in CCMS will now be directly visible to the end-users through the KSEMP**.**

H. Audit trail and logging

The Centralized Correspondence Management System (CCMS) shall incorporate a comprehensive audit trail and logging mechanism to ensure transparency, traceability, and accountability at every stage of communication processing. The system will automatically log all user activities and system events, including but not limited to, registration of communications, file creation, note and draft movements, approvals, dispatches, and system integrations. Each action will be timestamped and associated with the unique user ID and IP address (where applicable), enabling a complete chronological record of how a communication or file was handled from receipt to disposal. These logs will be protected from tampering and accessible only to authorized supervisory or audit personnel. The audit trail will support internal monitoring, compliance with statutory requirements, and efficient response to RTI queries, administrative reviews, or external audits. The system will also maintain logs of integration events with functional applications and external portals, ensuring that all data exchanges are recorded and verifiable. By embedding audit trails across all modules, CCMS reinforces a culture of accountability and provides a verifiable digital footprint for every transaction within the system.

I. Data Management (Storage, Retrieval, Backup)

The Data Management component of the Centralized Correspondence Management System (CCMS) is a critical architectural layer that ensures the secure, efficient, and scalable handling of all data generated, received, and processed within the system. This includes structured data (e.g., metadata, application logs, workflow states) and unstructured data (e.g., scanned documents, attachments, notes, and drafts). Effective data management ensures that communication records are persistently available, easily retrievable, and adequately protected from loss, corruption, or unauthorized access.

A. Data Storage Strategy

All data within CCMS shall be stored in a centralized, secure database hosted either in a government-approved cloud infrastructure or an on-premises servers, as per policy. The storage architecture shall be designed to support:

- **High availability and redundancy**, ensuring minimal downtime or data inaccessibility.
- **Structured storage** of transactional metadata and workflow logs within relational databases.
- **Unstructured storage** of scanned documents, PDFs, email attachments, and dispatch files in secure object/file storage systems.

Storage shall be logically segmented by module (e.g., online applications, offline entries, correspondence files), with proper indexing and tagging for fast retrieval and workflow mapping. All document files shall be retained in their original format and linked to their respective inward or file records.

B. Data Retrieval Mechanism

The CCMS will offer an efficient and responsive search and retrieval, as outlined in Section 3.7, allowing users to:

- Retrieve data by key identifiers such as Name, inward number, PEN, application type, subject, or date range.
- Access historical communication records, even after disposal or file closure, for reference, audit, or compliance checks.
- Open attachments, download scanned files, and view communication trails, based on user privileges.

Advanced indexing techniques shall be used to ensure low-latency retrieval of data, even under large-scale usage scenarios. The system will also support cross-module retrieval, enabling users to access linked records spanning multiple modules (e.g., an offline letter linked to a pension application).

C. Data Security and Access Control

To ensure data confidentiality, integrity, and availability:

- All storage locations shall be protected through encryption at rest.
- Data in transit (e.g., between CCMS and external platforms like KSEMP) shall be encrypted using SSL/TLS.

- Access to stored data shall be governed by **role-based access controls**, enforced through the user management module.
- Logs of all data access and file downloads shall be maintained for security auditing.

The system shall comply with relevant data protection and government IT policies, and periodic **data integrity checks** shall be conducted to detect corruption or unauthorized changes.

D. Data Backup and Disaster Recovery

A robust **automated data backup system** shall be implemented to protect all CCMS data from accidental loss, hardware failure, or cyber incidents. The backup policy shall include:

- **Daily incremental backups** of all databases and files.
- **Weekly full backups** stored at secure alternate locations or cloud storage.
- **Disaster recovery protocols**, allowing the system to be restored to a consistent state within a predefined Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Annexure II Non-Functional Requirements.

A Performance

The performance of the **Centralized Correspondence Management System (CCMS)** is critical to ensure smooth, uninterrupted communication management across multiple sections, branches, and modules operating concurrently. Given the system's layered architecture handling online applications, offline submissions, email diarisation, internal file workflows, and API-based integration , the CCMS must be designed to deliver **high responsiveness, low latency, and scalable throughput** under both regular and peak workloads.

The system must be capable of **simultaneous multi-user access** without performance degradation. It should efficiently manage concurrent tasks such as communication registration, real-time dashboard rendering, file creation, document uploads, and background status synchronization with functional applications (e.g., GPF Module, GEMS, P-SAI, VLC) and external platforms like KSEM Portal.

Key performance expectations include:

- **System Responsiveness**: The application should respond to standard user actions (login, file opening, document viewing) within 2–3 seconds under normal load conditions.
- **Concurrent User Handling**: The system shall support at least **500 concurrent users** during peak hours across Main Office and Branch Offices, with scalable backend support for higher loads as required.
- **Throughput Capacity**: The system should be able to process and register a minimum of **2000 communications per day** across modules without delay or bottleneck, including document scanning and file uploads.
- **Integration Latency**: The API integration with functional software and the Middle Server should ensure that status updates and document transfers occur within **5 seconds** of transaction completion in either system.
- **Dashboard Refresh and Reporting**: Real-time dashboards and summary MIS reports should load or refresh within **5 seconds** for average data volumes and within **10 seconds** for high-volume queries or filters.

- **Dispatch Recording and Status Closure**: Final dispatch entry and status change should be completed and confirmed in the system within **3–5 seconds** of action.
- **System Uptime**: The CCMS shall maintain a minimum of **99.8% system uptime**, excluding scheduled maintenance windows, ensuring uninterrupted operational availability for all users during working hours.
- **File Upload Handling**: The system shall support individual file uploads (PDFs,Word,Excel,Jpeg scanned documents) of up to **20 MB** per communication, with compression and indexing mechanisms to maintain speed and accessibility.

B. Security

Security is a foundational non-functional requirement for the Centralized Correspondence Management System (CCMS), which handles sensitive government communications, personal employee data, entitlement records, and audit-critical workflows. The system must incorporate multi-layered security controls that ensure confidentiality, integrity, availability, and accountability across all modules, users, and integrated platforms.

The CCMS shall adhere to the Government of India’s IT Security Guidelines and applicable departmental security protocols. It shall be protected against unauthorized access, data breaches, tampering, and misuse through a combination of application-level, data-level, and infrastructure-level security measures.

Key Security Requirements Include:

- **Role-Based Access Control (RBAC):**

Every user shall be assigned access privileges based on their designated role (e.g., DEO (Inward/dispatch section), Dealing Unit, Section Head, System Admin). Access to specific functionalities (view, edit, approve, dispatch) shall be tightly governed by these roles to prevent unauthorized actions.

- **User Authentication:**

All users must log in using secure credentials. Password policies shall enforce complexity, expiration, and reset protocols. Optionally, Two-Factor Authentication (2FA) may be implemented for high-privilege roles (e.g., Section Heads, Admins).

- **Data Encryption:**

All sensitive data shall be encrypted at rest and in transit. Communication between CCMS and external systems (e.g., KSEM Portal, GEMS, P-SAI) shall use secure protocols (e.g., HTTPS, SSL/TLS).

- **Audit Trails and Logging:**

As described in Section 3.11, all user actions including login attempts, document access, file movement, and dispatches will be recorded with timestamps and user IDs, IPs to enable traceability and review.

- **Access Session Control:**

User sessions shall auto-expire after a defined period of inactivity. Concurrent session limits and login alerts shall be implemented where necessary.

- **Security of Integration Interfaces:**

APIs used for interfacing with Middle Servers, GPF, GEMS, and KSEMP shall be **tokenized or authenticated** using secure methods. Only whitelisted endpoints shall be permitted to send or receive data.

- **Disaster Recovery and Data Protection:**

Backups shall be encrypted and securely stored. Restoration protocols shall ensure that data integrity and confidentiality are not compromised during recovery.

- **Security Monitoring and Alerts:**

The system shall include mechanisms to detect and alert abnormal usage patterns, repeated failed logins, or unauthorized data access attempts.

Compliance

The CCMS shall comply with:

- **Government of India's Cyber Security Policy** and guidelines issued by MeitY and CAG.
- Internal policies for **data retention, archival,** ensuring records are securely preserved and deleted when no longer required.

C Usability (User Experience – UX)

The **Centralized Correspondence Management System (CCMS)** shall be designed with a strong focus on **usability**, ensuring that users across all roles and levels—clerks, assistants, section heads, supervisory officers, administrators, and external stakeholders—can interact with the system **intuitively, efficiently, and with minimal training**. Given that the system replaces traditional manual registers, physical file movements, and fragmented workflows, it must offer a **user-centric interface** that simplifies complex processes and promotes rapid adoption across the organization.

Key Usability Objectives:

- **Simple and Consistent Interface Design:**

The user interface (UI) shall follow a clean and minimal design layout with consistent navigation patterns across all modules. Common user actions—such as registration, searching, viewing files, drafting, dispatching, and dashboard access—should be placed logically and remain easily accessible from the main dashboard or module-specific panels.

- **Role-based Dashboards and Workspaces:**

Each user will have a customized landing page tailored to their role. For example, inward clerks will see pending registrations and scanning queues; assistants will see assigned communications and open files; section heads will see files pending approval or review. This contextual UX reduces clutter and helps users focus only on their actionable items.

- **Guided Workflows and Status Indicators:**

The system shall incorporate clear visual indicators of file stages, processing status, pending tasks, and deadlines. Guided workflows, progress bars, and color-coded status markers will assist users in understanding where an item stands and what action is required next.

- **Search and Quick Navigation Tools:**

As outlined in Section 3.7, the system will support global search bars, filters, and saved queries, allowing users to retrieve communications quickly. Breadcrumb trails, back buttons, and shortcut keys shall be available to improve navigation speed.

- **Multi-device Compatibility (Optional/Future Scope):**

The system should ideally be responsive and accessible via desktops, laptops, and tablets used within the office network. This ensures flexibility for users working across different devices or sections.

- **Accessibility and Language Support:**

The interface shall comply with basic accessibility standards (e.g., readable fonts, contrast levels, keyboard navigation) and may optionally offer support for local language display where appropriate (e.g., Malayalam labels for scanned communications).

- **Error Prevention and Feedback:**

The system shall offer real-time validation for data entry, prevent accidental duplicate entries, and provide user-friendly error messages. Successful actions (e.g., registration completed, file submitted) shall be acknowledged with confirmation messages.

D. Scalability

The **Centralized Correspondence Management System (CCMS)** shall be designed as a **modular, extensible, and future-ready platform**, capable of supporting the growing needs of the office over time. The system must accommodate increases in users, volume of communications, data size, integration points, and administrative jurisdictions—without requiring significant reengineering or performance degradation. Additionally, the architecture shall support easy maintenance, upgrades, and enhancements with minimal service disruption.

Scalability Requirements:

- **User Scalability:** The system shall support a growing number of simultaneous users, extending from the initial user base in the Main Office and existing Branch Offices to future users in additional administrative units or new sections, if created. The backend must handle a projected increase in concurrent sessions without impact on speed or stability.
- **Data and Transaction Scalability:** CCMS shall be able to manage increasing volumes of communications (online applications, offline submissions, correspondence files) over time. The system should handle thousands of new records per month and millions of cumulative archived communications with no compromise in retrieval performance.
- **Modular Expansion:** The architecture shall follow a loosely coupled modular design, allowing new features, workflows, or communication categories to be added without affecting the functioning of existing modules. Future functional modules—such as departmental circular tracking, stakeholder grievance modules, or external integrations—should be accommodated smoothly.
- **Infrastructure Elasticity:** If hosted on cloud or hybrid infrastructure, the system must support **scaling** of server resources (processing, memory, storage) as per workload demands. If hosted on-premises, hardware sizing and storage planning must allow expansion without major redesign.

E. Data Integrity and Validation

The **Centralized Correspondence Management System (CCMS)** shall enforce strong **data integrity and validation mechanisms** across all modules and transactions to ensure the accuracy, consistency, and trustworthiness of communication records throughout their lifecycle. Since the system handles official correspondence, entitlement applications, authorizations, and workflow-based approvals, even minor data anomalies can lead to miscommunication, delays, or audit non-compliance. Therefore, data entered, imported, or exchanged must be rigorously validated, structured, and protected from unauthorized or accidental modification.

A. Data Integrity Controls

- **Transaction-Level Integrity:**Each communication registered in the system—whether online, offline, or through email—will be uniquely identified and linked to a permanent **inward number**, ensuring no duplication or overwriting. All transactions, including status updates, file movements, and dispatches, must follow strict update rules backed by timestamps and user IDs.
- **Relational Consistency:** Data models will enforce relational integrity, ensuring that every file, communication, or note is linked to its parent section, functional module, or registered user. The system will prevent orphan records or dangling references that can compromise reporting or traceability.
- **Immutable Logs:** Historical actions, such as who registered a communication, who drafted and approved a file, and when it was dispatched, shall be stored in immutable audit logs to prevent retroactive tampering or deletion.
- **Change Detection and Alerts:** The system shall monitor critical fields (e.g., PEN, acknowledgment number, application type) for unauthorized changes and alert supervisors or administrators when inconsistencies or rollback attempts are detected.

B. Data Validation Mechanisms

- **Form-Level Validation:** All user entry forms such as inward registration, file creation, note drafting, and email diarisation, dispatch shall include input validation checks for required fields, data types, length, format (e.g., valid PEN, date), and allowed values.
- **Pre-Processing Checks:** For online applications received via Middle Server or external APIs, the system will verify incoming data against pre-defined validation rules before accepting them into the CCMS database. Invalid or incomplete records shall be rejected with appropriate error messages and logged for follow-up.
- **Duplication Prevention:** The system shall automatically detect and prevent duplicate registrations using identifiers such as acknowledgment number, PEN, and inward date. When a potential match is found, the user will be prompted to review the existing record before proceeding.
- **Attachment Validation:** Uploaded documents will be scanned for file type, size, and security compliance. Corrupted or disallowed file formats shall be flagged and rejected at the time of upload.
- **Data Synchronization Integrity:** In integration scenarios with functional applications and portals (e.g., GPF Module, GEMS, KSEMP), the system will ensure that all sent and received

data matches expected formats and values. Mismatches or sync failures shall trigger alerts and retry mechanisms to ensure complete and accurate exchange.

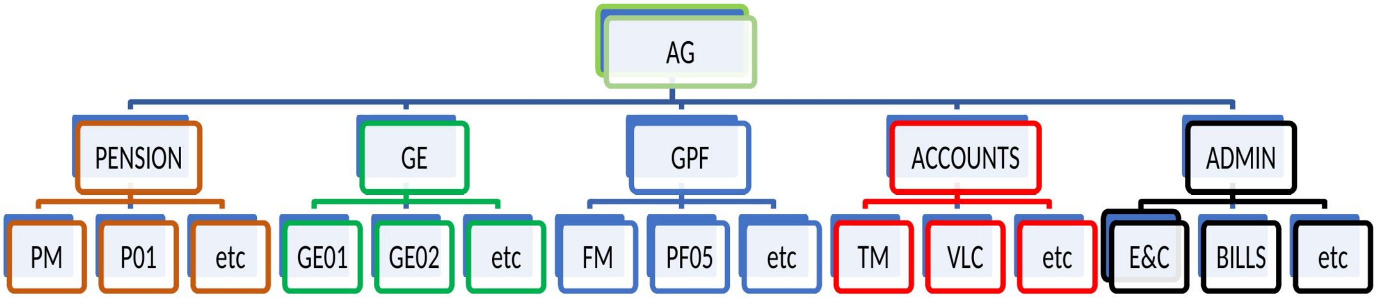
Annexure – III - Glossary / Definition

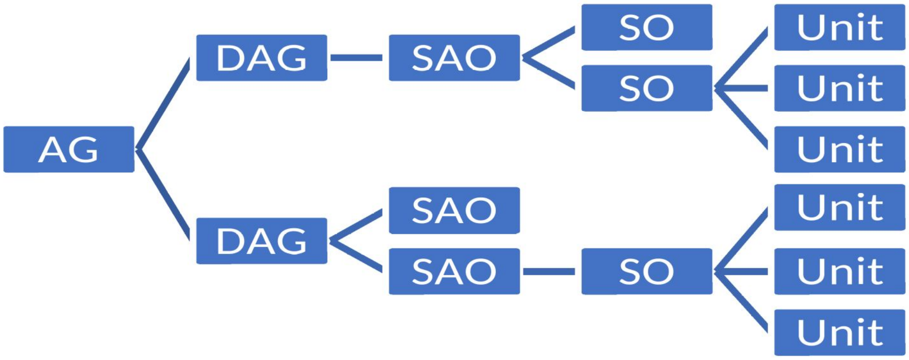
Term / Abbreviation	Definition
2FA	Two-Factor Authentication – Security mechanism requiring an additional verification step (e.g., OTP/email confirmation).
Audit Trail	A chronological log that records user actions and system events for each communication/file for transparency and accountability.
CCMS	Centralized Correspondence Management System – The proposed software solution providing a unified digital platform for managing all categories of communications across the office.
Dashboard	A real-time interface showing pending, processed, and closed communications across sections and modules.
Dispatch	The final step in a communication's lifecycle, where the approved reply or authorization is sent to the stakeholder via email, post, or integrated portals.
Email Diarisation	The process of auto-registering or manually capturing incoming email communications into CCMS.
File Workflow	The movement of digital files within CCMS from one user/role to another, with note preparation, draft generation, and approval tracking.
Functional Applications	Internal systems used for entitlement processing (e.g., GPF Module, GEMS, P-SAI, VLC) that are integrated with CCMS for status synchronization.
GEMS	Gazetted Entitlement Management System – Manages Pay and Service particulars of Gazetted Officers of State Government.
GPF Module	Application used to manage General Provident Fund cases – advances, final withdrawal, and subscriptions.
Inward Number	A unique identifier generated by CCMS at the time of registering a communication or application, used for internal tracking and reference.
KSEM Portal /	Kerala State Employee Management Portal – External portal where government

KSEMP	employees submit applications and track entitlement status.
Middle Server	An intermediate software layer that transfers online applications from external portals (e.g., SPARK, Treasury application) to internal processing systems.
MIS	Management Information System – Dashboard and report modules in CCMS that provide section-wise summaries, pendency reports, and performance analytics.
Note / Draft	Internal documents generated in response to a communication: “Note” for justification; “Draft” for proposed reply or order.
Offline Communication	Any communication or application received via post, hand delivery, or non-integrated email sources.
Online Application	Digital entitlement application submitted via stakeholder portals and routed through Middle Servers.
P-SAI	Pension – System Automation Initiative – Module for pension processing and authorization.
RBAC	Role-Based Access Control **–** Access permissions assigned based on user roles (e.g., Clerk, Assistant, Section Head).
Status Synchronization	Automatic real-time reflection of status updates from integrated functional systems into CCMS.
VLC	Voucher Level Computerisation – Module used in Accounts Wing to manage data related to the accounts of State Government.

Annexure IV

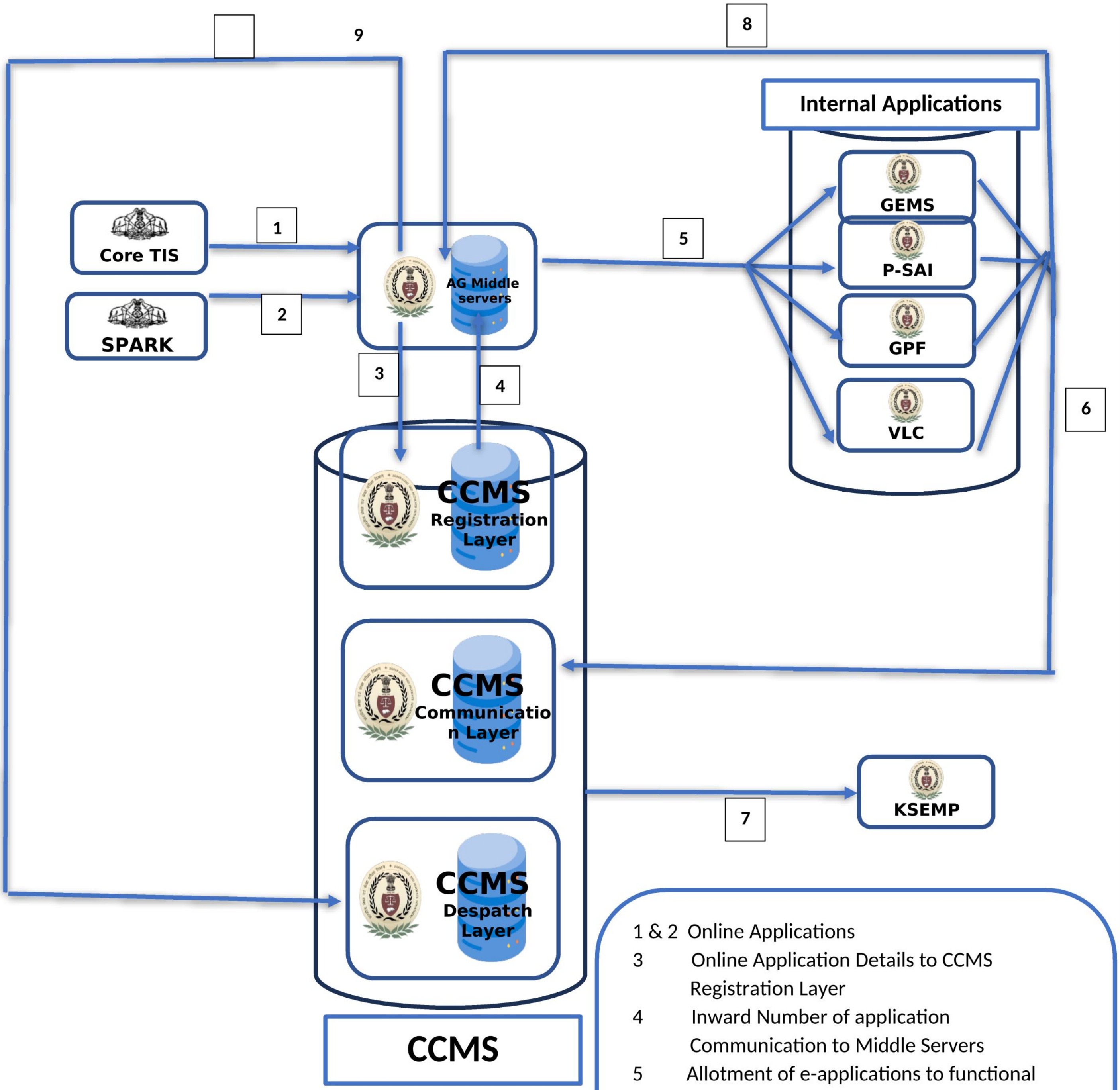
Organizational Structure





Annexure V

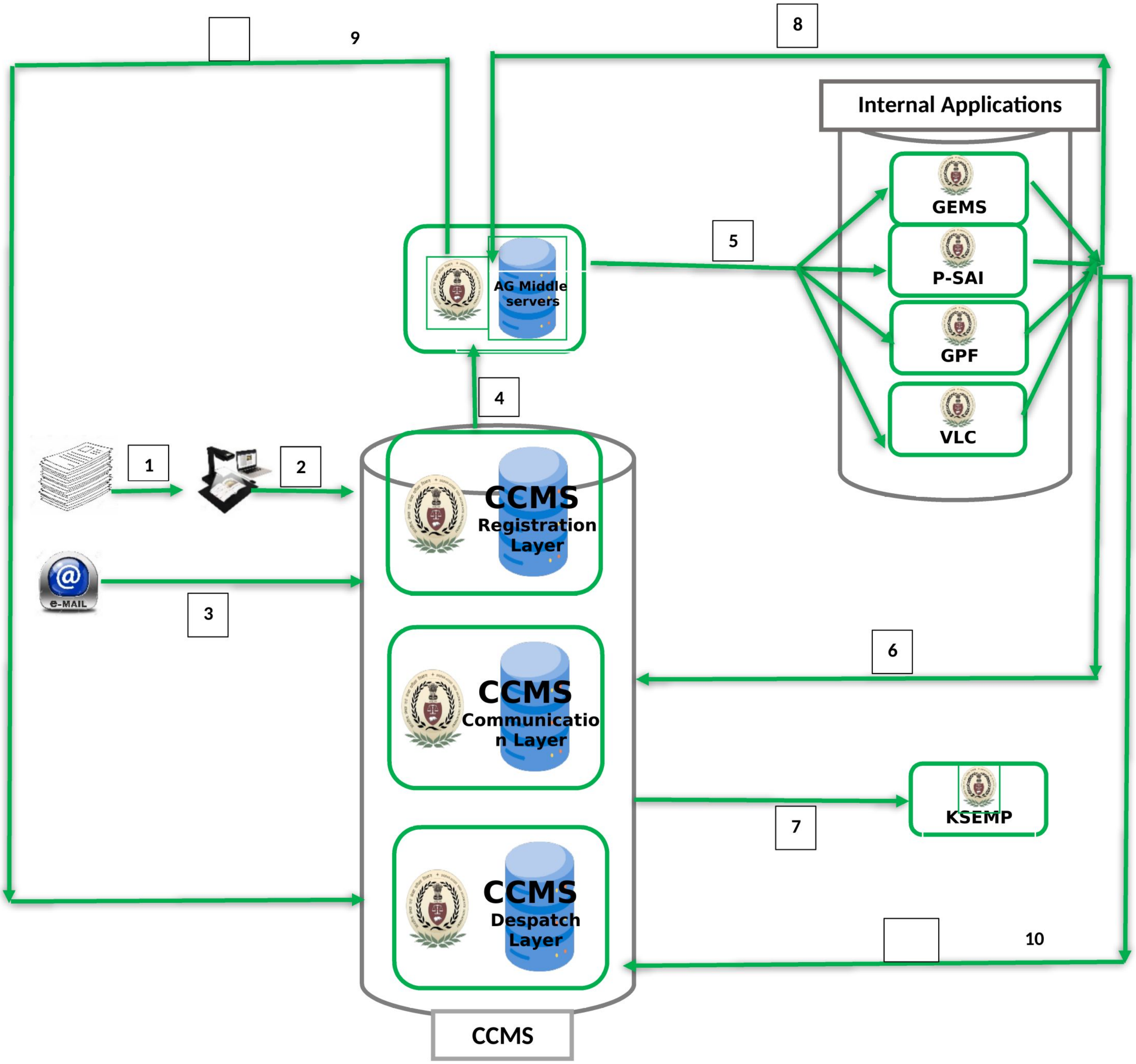
Online Applications Workflow -Schematic Representation



1 & 2 Online Applications
3 Online Application Details to CCMS Registration Layer
4 Inward Number of application Communication to Middle Servers
5 Allotment of e-applications to functional applications
6 Realtime status of e-application to CCMS
7 Realtime status of e-applications to KSEMP
8 E- Authorization to Middle Servers
9. Dispatch Status Updation to CCMS

Annexure VI

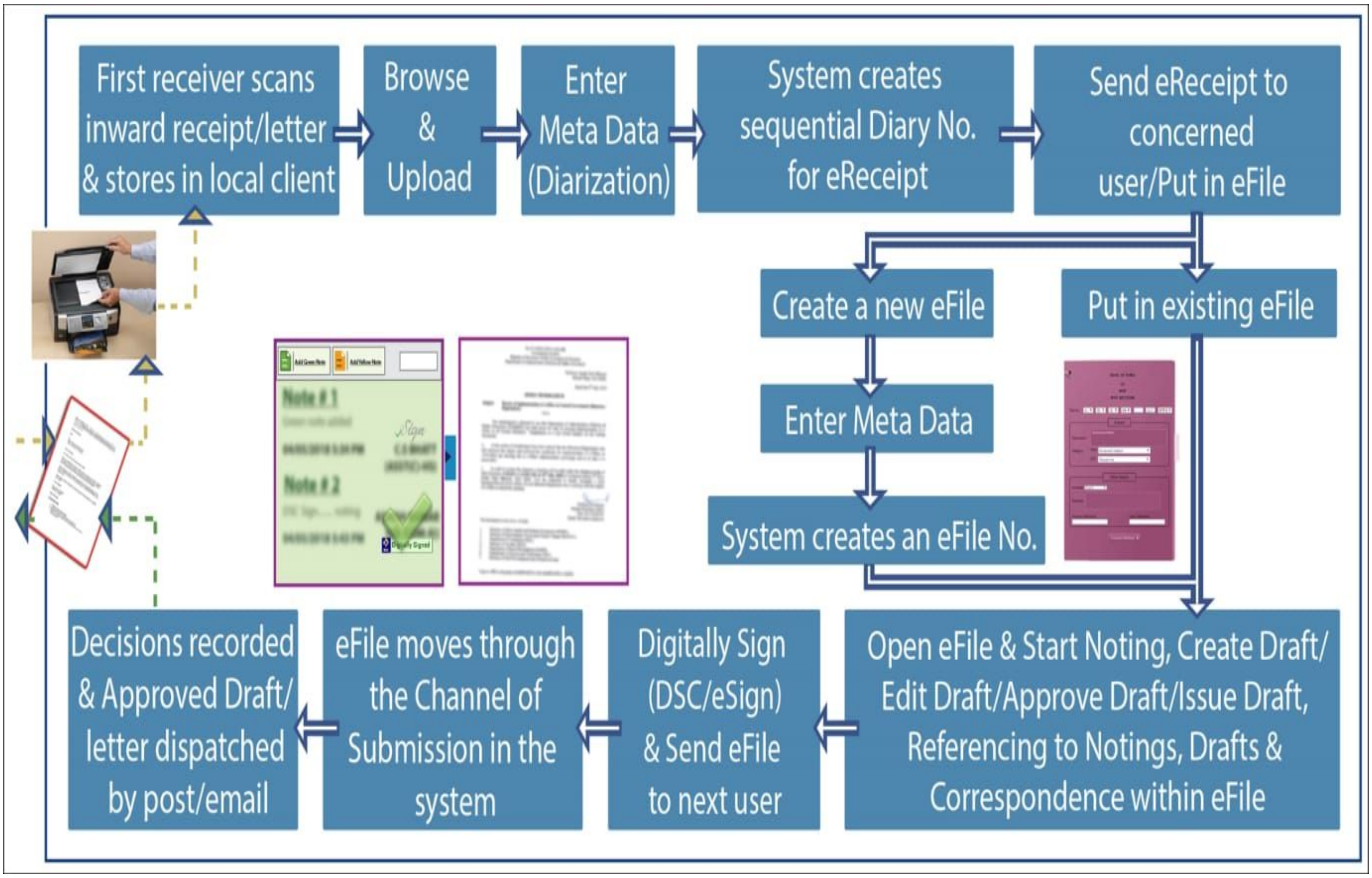
Offline Applications Workflow -Schematic Representation



1 Physical Documents Scanning
2 Scanned Document Uploading in CCMS Registration Layer
3 Email Diarization in CCMS Registration Layer Registration Layer
4 Application pushing to Middle Servers
5 Allotment of e-applications to functional applications
6 Realtime status of application to CCMS
7 Realtime status of e-applications to KSEMP
8 E- Authorization to Middle Servers
9 Dispatch Status Updation to CCMS
10 Physical / Email dispatch to Despatch Module of CCMS

Annexure VII

Correspondence Management Layer-Schematic Representation


First receiver scans inward receipt/letter & stores in local client
Browse & Upload
Enter Meta Data (Diarization)
System creates sequential Diary No. for eReceipt
Send eReceipt to concerned user/Put in eFile
Create a new eFile
Put in existing eFile
Enter Meta Data
System creates an eFile No.
Note # 1
Note # 2
Open eFile & Start Noting, Create Draft/ Edit Draft/Approve Draft/Issue Draft, Referencing to Notings, Drafts & Correspondence within eFile
Digitally Sign (DSC/eSign) & Send eFile to next user
eFile moves through the Channel of Submission in the system
Decisions recorded & Approved Draft/ letter dispatched by post/email