CMS — Contraband Management System — Final System Overview & Complete Plan

Below is the final, production-ready plan for CMS: a complete, detailed description of architecture, roles, pages, every major button/option, workflows, APIs, security, deployment, testing, and runbooks. It's organized for engineers, product owners, and implementers so you can hand this to a dev team and start building.

1 — Executive Summary

CMS provides the Ethiopian Federal Police a secure, auditable, mobile-first system to register, track, store, transfer, and destroy seized contraband. Key guarantees: tamper-evident chain-of-custody, legal-grade evidence packets, fast field capture (PWA with offline), RBAC + MFA, and auditable destruction workflows.

2 — Users & Roles (full detail)

Each role lists default permissions and example UI scope.

Admin

Permissions: Full system-wide CRUD, user & role management, system settings, audit log access, export rights, backup/restore, grant guest access.

Sensitive: Can change retention policy, KMS/Vault settings, and revoke access.

Supervisor

Permissions: Approve/Reject custody transfers & destruction requests; view & edit contraband non-critical fields (where allowed); view dashboards & compliance reports; flag incidents.

Warehouse Manager

Permissions: Acknowledge receipt; manage storage location inventory; perform audits; create inventory adjustments; scan barcodes/RFID.

Field Officer

Permissions: Create seizure records; attach photos/docs; initiate custody transfers; view own items; sync offline captures.

Auditor

Permissions: Read-only access to audit logs and evidence packets; generate and export reports; flag anomalies (readonly on records).

Guest / External Auditor

Permissions: Time-limited, read-only access to selected cases or exported packets (granted by Admin).

System (Service Account)

Permissions: For internal integrations (e.g., messaging webhook, barcode printer service). Managed in Vault.

3 — Final Architecture (short recap)

Frontend: React + TypeScript (PWA for Field Officers).

Backend: Java Spring Boot microservices:

Auth Service (OAuth2/OIDC, JWT, MFA)

User & Roles Service

Contraband Service

Custody Service

Inventory Service

Destruction Service

Notification / Messaging Service

Audit Service (append-only)

Data: PostgreSQL (+ PostGIS), Redis, S3-compatible object-store (encrypted), Elasticsearch (optional)

Messaging: Kafka or RabbitMQ

Infra: Docker, Kubernetes, CI/CD, Vault/KMS, Prometheus/Grafana, EFK (logging)

Security: TLS 1.2+, AES-256 at rest, WAF, SAST/DAST, scheduled pen-tests

Backups: Daily DB backups + offsite object store replication + WAL archiving

4 — Full UI Map: Pages, Components, Buttons & Options

Below each page includes: primary purpose, fields, buttons, options, workflows, and confirmations.

Note: icons (e.g., 🔍, 📸) are optional UI affordances to improve UX.

A — Global UI elements

Top nav: Logo | App name | Global search (contraband code / serial / officer) 🔍 | Notifications bell (badge) | User avatar (menu: Profile, Preferences, Help, Logout)

Left sidebar (role-based): Dashboard, Seizures, Inventory, Transfers, Destruction, Audit Logs, Reports, Admin, Help

Footer: Version, Last sync time (PWA), Environment (DEV/STAGE/PROD)

Floating Action Button (FAB) (Field Officers): “New Seizure” (+)

Contextual action toolbar on lists (multi-select actions)

B — Login & Auth Screens

Login Page

Fields: Username / Email, Password

Buttons: [Sign In], [Forgot Password], [Use MFA Token]

Options: “Remember me” (only local device cookie), Language toggle (EN / AM)

Constraints: Block after 5 failed attempts (configurable)

UI messages: success, invalid credentials, locked account

MFA Verification

Methods: TOTP (authenticator app), SMS OTP (configurable)

Fields: 6-digit code

Buttons: [Verify], [Resend SMS] (rate limited)

Options: “Remember this device” (expires after configurable days)

Password Reset

Flow: Request → Email token → Reset form

Buttons: [Send Reset Link], [Reset Password]

Validations: token expiry, password strength

C — Dashboard (role-dependent)

Purpose: Snapshot of key KPIs and quick actions.

Widgets (configurable):

Today's seizures (count) → click to filter list

Pending transfers → [View Transfers]

Pending destruction requests → [View Destructions]

Recent audit flags → [View Audit]

Inventory health (by location) → heatmap or list

Buttons:

[New Seizure] (Field Officers & Supervisor via FAB)

[Generate Report] (Admin/Supervisor) → modal to configure filters, schedule

[Export Dashboard CSV/PDF] (Admin)

Options:

Widget settings (gear icon): show/hide, reorder, time range

D — Seizure Registration Page (Field Officer PWA, core page)

Purpose: Capture seizure details in ≤ 5 taps when possible.

Form layout (compact)

Header

Title: “Register Seizure”

Buttons: [Save Draft], [Submit Seizure], [Cancel]

Draft autosave indicator

Primary Fields (top row)

Contraband type (dropdown) — required

Category (dropdown) — required

Quantity and unit — required (number + unit dropdown)

Serial number / identifier (text)

Contraband code (auto-generated on submit, preview shown after save)

Seizure Details

Seizure time (auto-now, editable)

Seizure location (GPS): [Capture GPS] button → fills lat/lon and map preview

Location type (dropdown): road, checkpoint, home, market, vehicle, other

Seized by (auto-filled officer account, editable if supervisor)

Agency (text/dropdown)

Notes (multi-line)

Media & Documents

Photo capture area: [Take Photo] (opens camera), [Upload Photo] (file)

Documents: [Attach Document] (PDF / DOC)

Media thumbnails with trash/delete icon, reorder handles

Options: redact/blurring tool for photos (simple blur tool client-side)

Chain-of-custody initial state

Storage assignment (dropdown, optional at registration)

Initial custody status (Registered / Handed to Warehouse Pending)

Checkbox: “Item physically handed to ______” → opens transfer init flow

Buttons behavior

[Save Draft] — saves local and server draft when online

[Submit Seizure] — validates required fields, uploads media, generates UUID + contraband_code, enqueues notification to Supervisor, logs audit event

Confirmation modal: “Submit seizure — once submitted, core fields require Supervisor changes” [Confirm / Cancel]

[Cancel] — discard draft confirmation: [Yes discard / Keep draft]

Offline specifics

If offline: show “Offline — saved locally” badge, [Sync Now] button when online

Sync conflict resolution modal if same item edited elsewhere

E — Contraband List & Search Page

Purpose: Search, filter, bulk actions.

Search bar: text search (contraband_code, serial, description)

Filters: status, type, category, date range, location, assigned storage, seized_by, agency

Columns: checkbox, contraband_code, thumbnail, type, quantity, status badge, seizure_time, assigned_storage, actions

Actions per row:

[View] → open detail drawer

[Edit] (allowed roles) → opens edit modal or page

[Initiate Transfer] → opens transfer modal

[Request Destruction] → opens destruction modal

[Generate Barcode] → shows printable label modal

[Export Evidence Packet] (Admin/Auditor) → generates ZIP/PDF evidence

Bulk actions (toolbar):

[Bulk Transfer], [Bulk Export], [Bulk Generate Labels], [Bulk Assign Storage], [Bulk Delete Drafts] (Admin only)

Pagination & page size control

Sort options on columns

Keyboard shortcuts: select all, open first result (optional)

F — Contraband Detail Page (single item)

Sections

Header

Title: Contraband #{contraband_code} — status badge

Buttons: [Print Label], [Generate Evidence Packet], [Add Note], [Flag], [Edit (if permitted)], [Lock Record (Admin)]

Quick actions: [Initiate Transfer], [Request Destruction], [Scan/Rescan]

Summary Card

Key fields: type, category, qty, units, serial, seized_by, seizure_time, seizure_location (mini-map), assigned_storage

Photo carousel — click to enlarge, download, redact/download redacted

Tags: case number, related cases (links)

Custody Timeline

Chronological list of custody events (created by Audit Service)

Each event shows: actor, action, timestamp, geolocation (if applicable), notes, supporting media thumbnail

Buttons per event: [View Evidence], [Comment]

Storage & Inventory

Current storage location card with [Navigate] link, [Print Storage Label]

Transfer history & pending transfer widget

Destruction Panel

If destruction requested: show approvals, schedule, witnesses

Buttons: [Request Destruction], [Cancel Request] (if allowed), [Force Destroy (Admin only)]

Audit & Chain-of-Custody

Hash & verification status (computed by Audit Service)

Button: [Verify Integrity] → shows SHA chain details and anchor status (offsite anchor)

Notes & Comments

Freeform comments with roles & timestamps; attachments allowed

Buttons: [Add Note], [Resolve Note]

Activity & Logs

Events: edits, access logs (who viewed), export events

Button: [View Access Log]

G — Transfer Workflow UI (Custody)

Initiate Transfer Modal

Triggered from list/detail page.

Fields:

From location (auto)

To location (dropdown)

Requested by (auto)

Reason (text) — required

Attachments (photos/signatures)

Urgency (normal / urgent)

Buttons: [Request Transfer], [Save Draft], [Cancel]

Post-request:

Notification to Supervisor(s)

Transfer enters “Pending Approval” status

Supervisor Approval Page

List of pending approvals

Buttons per request: [Approve], [Reject], [Request More Info]

Approval modal: Approver adds note, can mark scheduled pickup time

After approve: notification to Warehouse Manager with pickup details

Warehouse Receipt Flow

Warehouse Manager sees “Incoming Transfers”

Options: [Acknowledge], [Reject]

On acknowledgement: scan barcode (or manual accept) → Receiver signature capture (digital signature via touch/camera)

Updates custody status; audit event logged

Buttons & confirmations

[Approve] → confirmation modal (record approver & timestamp)

[Reject] → reason required

[Acknowledge] → upload receipt photo, signature capture

H — Inventory & Scanning UI

Inventory Location Page

Location header: name, address, capacity, contact

Inventory list: items assigned to location

Buttons: [Start Inventory Audit], [Scan Item], [Export Location Report]

Scan Interface

Input: Barcode scanner integration (hardware) or manual barcode entry

Actions after scan:

Show item mini-card → [View], [Mark Found], [Mark Missing], [Reassign]

Bulk scan mode: continuous scanning with counts

Discrepancy handling: if missing, register incident → notifies Supervisor & Auditor

Inventory Audit Flow

Start audit → assign auditor/participants → scan expected list or full scan

Buttons: [Start], [Pause], [Finish]

On finish: generate audit report (CSV/PDF) and discrepancy list

I — Destruction Workflow UI

Request Destruction Modal

Initiator (Supervisor usually)

Fields:

Items (multi-select contraband)

Reason & legal basis (text, required)

Proposed method (dropdown: incineration, chemical neutralization, crushing, other)

Proposed schedule (date/time)

Witnesses (list of user accounts + external names)

Attach supporting docs/photos

Buttons: [Request Approval], [Save Draft], [Cancel]

Approval Chain

Multi-level approval UI:

Each approver sees [Approve] / [Reject] with comment

Approvals displayed with timestamps & digital signatures

Upon final approval:

Schedule popup: [Complete Destruction] action for the Warehouse Manager / Destruction Team

Destruction Event Logging

On-site: capture photos/videos, witness signatures (digital), method confirmation

Buttons: [Start Destruction], [Log Event], [Complete Destruction]

After completion: system generates destruction certificate (PDF) with SHA, printed label, and archival in Object Store

Audit: destruction event creates immutable log and evidence packet

Critical confirmations

Before [Complete Destruction]: modal “This action is irreversible. Confirm destruction of N items.” with typed confirmation (type “DESTROY” or contraband code)

After completion: final state set to destroyed and cannot be edited except Admin (with strict audit trail)

J — Audit Logs & Reports UI

Audit Log Page

Filters: entity_type, entity_id, action, actor, date range, location

Logs shown with cryptographic hash column; verify button

Buttons: [Export Logs], [Flag], [Request Review]

Detail view: shows metadata_json, linked media, hash chain proof

Reports Page

Pre-built reports: Daily Seizures, Pending Transfers, Destruction History, Location Inventory, Audit Exceptions

Generate options:

Filters: date range, location, officer, status

Output: PDF, CSV, ZIP evidence packet (select)

Scheduling: schedule recurring report with recipients

Buttons: [Generate Now], [Schedule], [Save Template]

K — Admin Console UI

Users & Roles

List users with status, last login, role

Buttons: [Create User], [Edit], [Disable], [Reset Password], [Enable MFA], [Assign Role], [View Activity]

Create user modal fields:

Username, display name, email, phone, role (multi-select for role groups), agency, station

Initial password (auto-generated), require password change on first login

Options: force MFA, set account expiry

System Settings

Tabs: General, Security, Notifications, Retention, Integrations

Options:

General: system name, language default, branding, timezone

Security: password policy, lockout threshold, session timeout

Notifications: default channels, provider config (SMTP, Twilio, in-app), retry policies

Retention: default retention periods per category (contraband type), auto-purge options

Integrations: SSO/OIDC config, Barcode printer endpoints, SMS gateway, Webhooks

Buttons: [Save Changes], [Test Connection] for providers, [Reset to Defaults]

Locations Management

CRUD for storage locations with map pin, capacity, contact info

Buttons: [Add Location], [Edit], [Deactivate], [Set as Default Receiving Point]

Secrets & Keys

Admin sees placeholders; actual secrets in Vault

Buttons: [Rotate Key], [Test Key], [Audit Key Usage]

Option: export service account keys (Admin-only, time-limited download)

Backups & Restore

Buttons: [Trigger Backup], [List Backups], [Restore] (restore requires 2 Admin confirmations)

Options: schedule backup window, retention

L — Notifications Center (In-app)

Bell opens list of notifications (filter: all/unread)

Notification item shows icon, title, timestamp, link to resource

Buttons:

[Mark as Read], [Snooze], [Open], [Manage Preferences] (opens profile preferences)

Notification preferences (Profile):

Toggle channels (Email / SMS / In-app), schedule (do not disturb hours), urgent-only toggles

M — Profile & Preferences

Profile info: name, email, phone, agency, station

Buttons: [Edit Profile], [Change Password], [Enable/Disable MFA], [Download Personal Activity Log]

Preferences:

Language, timezone, notification channels, default landing page

Device management: list of remembered devices, revoke

5 — Full Workflows (end-to-end)

1. Seizure → Storage → Audit (simple flow)

Field Officer: [New Seizure] → fill form → [Submit Seizure]

System: generate UUID & contraband_code; upload photos; create audit event; notify Supervisor

Supervisor: receives notification → [Approve Transfer] (if field officer requested)

Warehouse Manager: receives transfer notice → [Acknowledge], scans barcode on receipt

Item status updates to in-storage; inventory updated; audit log entry

2. Transfer with multi-step approval

Initiator requests transfer → status pending_approval

Supervisor approves → status approved

Warehouse scheduled pickup → Warehouse Manager [Acknowledge]

Receiver signs on receipt; custody transfer finalised; audit logged; notifications sent

3. Destruction (compliance-heavy)

Supervisor creates destruction request with legal basis → multi-level approval sequence

Each approver signs digitally → audit chain

Once fully approved: schedule destruction; on-site capture of photos & witness signatures

Warehouse Manager marks completed → system generates destruction certificate

Evidence packet is archived; item status destroyed

4. Audit & Anomaly

Auditor flags mismatch (e.g., missing item)

System triggers incident workflow: lock record, auto-notify Supervisor & Admin, trigger inventory audit job

6 — API Specification (selected, final)

All APIs require JWT auth. Use OpenAPI spec for full definition.

POST /api/auth/login → tokens

POST /api/auth/mfa/verify

GET /api/users, POST /api/users, PUT /api/users/{id}, DELETE /api/users/{id}

POST /api/contraband — multipart: metadata + photos

GET /api/contraband — filters

GET /api/contraband/{id}

PUT /api/contraband/{id} — restricted fields

POST /api/contraband/{id}/generate-barcode

POST /api/custody-transfers — request

PUT /api/custody-transfers/{id}/approve

PUT /api/custody-transfers/{id}/receive

POST /api/destruction-requests

PUT /api/destruction-requests/{id}/approve

POST /api/destruction-events

GET /api/audit — filters

POST /api/reports/generate

POST /api/notifications/send — internal

POST /api/inventory/scan — barcode/RFID update

Webhook endpoints

POST /api/webhooks/sms-delivery — SMS gateway callbacks

POST /api/webhooks/printer-status — barcode printer status

7 — Data Model Summary (core entities — final)

User(uuid, username, display_name, email_enc, phone_enc, role_id, station_id, active, mfa_enabled, created_at)

Role(id, name, permissions_json)

ContrabandItem(id UUID, contraband_code, type, category, description, quantity, unit, serial_number, seizure_time, seizure_location (geom), seized_by_user_id, photos[], documents[], status, assigned_storage_id, created_at, updated_at)

StorageLocation(id, name, address, location geom, type, capacity)

CustodyTransfer(id, contraband_id, from_location_id, to_location_id, requested_by, requested_at, approved_by, approved_at, received_by, received_at, status)

DestructionRequest(id, contraband_ids, requested_by, requested_at, approvals[], scheduled_time, method, witnesses[], photos[], status)

AuditLog(id, actor_user_id, action, entity_type, entity_id, timestamp, metadata_json, hash)

Notification(id, type, recipients[], payload_json, sent_at, status)

Indexes: contraband_code (unique), serial_number, status, seizure_time, assigned_storage_id, spatial indexes on geom fields.

8 — Security (full detail)

Authentication: OAuth2 Authorization Code + PKCE for native clients; JWT access tokens (short lived), refresh tokens rotated.

MFA: Required for Admin & Supervisor; encouraged for other roles.

Encryption:

TLS 1.2+ for all transport.

AES-256 for database fields (PII) and S3 objects encrypted with KMS.

Key Management: Vault or Cloud KMS with key rotation.

Audit Integrity: AuditService chains SHA-256 hashes, periodically anchors to offsite immutable store (e.g., timestamping service or blockchain anchor).

RBAC: Enforce at API gateway and service layer.

Operational: WAF, rate limiting, CSP, security headers, SAST/DAST, dependency SCA.

Admin protections: IP allow-list for admin console, step-up authentication for sensitive actions.

Data retention: Configurable retention policies; secure purge flows (soft-delete + final delete with admin override).