# NatioID - Updated Version (Citizen, Admin, SuperAdmin, RBAC, API, Security, DevOps)

## Original Content (from uploaded file)

NATIOID  
📖 NatioID – Citizen App Pages & Features   
  
📐 Layout System  
Citizen Layout  
Public Layout: Welcome, About, T&Cs.  
Auth Layout: Login, Forgot PIN, OTP.  
App Layout (post-login):  
Header (logo, quick access, notifications).  
Bottom Navigation (Home, Benefits, ID, More).  
Optional footer (support, app version).  
Admin Layout  
Sidebar Nav: Dashboard, Citizens, Elections, Benefits, Settings.  
Topbar: Admin name, role, logout/settings, global search.  
Main Area: Dynamic content with cards/tables/graphs.  
Key Difference: Sidebar-driven (for complex navigation) vs. bottom-nav (citizen side).  
🚀 First-Time Onboarding Flow  
Splash Screen  
App logo + animation.  
Prepares resources (language, user status).  
Language Selection Page (first-time only)  
Languages: English, Yoruba, Hausa, Igbo, Pidgin (expandable later).  
Stored in user profile, can change in Settings.  
Welcome / Intro Page  
Explains purpose of NatioID (security, ID, services).  
Swipeable slides or static info.  
Registration Page  
Methods: NIN (primary), BVN, Phone/Email.  
Collect: Full name, DOB, phone, email.  
Create 4–6 digit PIN.  
Optional selfie upload.  
OTP Verification Page  
Enter OTP via SMS/Email.  
Retry + change delivery method.  
Biometric Setup Page  
Fingerprint / FaceID setup.  
Skip option (enable later in Settings).  
Digital Consent / Terms Page  
Accept T&Cs, privacy & data-sharing consent.  
Success / Confirmation Page  
“Welcome to NatioID” message.  
CTA → Go to Dashboard.  
  
🔁 Returning User Flow  
Splash Screen – loads resources, directs to login.  
Login Gateway Page – PIN login (default) + Biometric (if enabled).  
“Forgot PIN?” → Account Recovery.  
Account Recovery Page  
Reset PIN via OTP/email/NIN verification.  
Option to re-enable biometric login after reset.  
Verification Status Page  
States: Pending / Verified / Rejected.  
Guidance for rejected cases.  
Dashboard / Home Page – main entry point after login.  
  
🧭 Core Citizen Functionality  
My ID (Digital ID Wallet)  
Profile picture, name, DOB, NIN, QR/Barcode.  
Download/Share ID securely.  
Offline access supported.  
Profile Settings Page  
Edit non-core details (phone, email, address).  
Manage PIN, biometric login, recovery options.  
Linked Documents Page  
Driver’s license, passport, voter’s card, health insurance.  
Integration with gov databases.  
Application Tracking Page  
Track gov services applied for (passport, subsidies, benefits).  
  
📰 News & Updates  
Government Updates Feed Page – national policies, reforms, subsidies.  
Economic Dashboard (New) – market data, inflation, subsidies info.  
Notification Center Page – filter by: All, Security, Govt, Financial, Personal.  
  
📊 Civic & Benefits  
Voting Page – election info, dates, candidates, manifestos.  
Election Results & Candidate Profiles – real-time results + transparency.  
Benefits & Subsidies Page – grants, pensions, healthcare, education.  
Status tracking + eligibility check.  
  
📡 Core Features  
Scan ID Page – QR/Barcode scanner for verifying citizens’ IDs.  
Print ID Page – generate/download printable ID format.  
Report Lost/Stolen ID Page – instantly flag ID + notify authorities.  
Digital Signature & Document Verification (New) – e-sign and validate gov docs.  
Activity Timeline Page – chronological log of actions (logins, votes, scans).  
  
⚠️ Safety & Security  
Security Alerts / SOS Page (New)  
Push alerts for emergencies.  
SOS button → send live location to authorities.  
Security Center Page  
PIN reset, biometric management, suspicious login alerts.  
Offline Mode  
Store essential ID data locally for verification when offline.  
  
⚙️ Utility & Personalization  
Settings Page  
Change language, theme.  
Security (PIN reset, inactivity lock).  
Accessibility (font size, high-contrast, screen reader, voice commands).  
Help & Support Page  
FAQs, chatbot, contact form, live chat (future).  
Complaint Tracking Page (New)  
Submit & track civic complaints (ID, benefits, services).  
Tutorials / Coach Marks Page  
Guided tour for new users.  
  
🛡 Cross-Cutting Enhancements (Global)  
Accessibility Features → screen reader, high contrast, large fonts, voice commands.  
Multi-language Support → Yoruba, Hausa, Igbo, Pidgin, English.  
Data Privacy & Transparency → dashboard showing stored data, who accessed it, permission controls.  
Real-Time Updates → push notifications for emergencies, elections, policy changes.  
Biometric Enhancements → multi-factor auth with biometric + PIN/OTP.  
Integration with Third Parties → banks, police, hospitals, tax.  
Usage Analytics & Guided Tips → improve UX and track adoption (admin only).  
User Activity Log → accessible under Activity Timeline.  
  
📌 Total Pages (Citizen side) → ~35  
(8 Onboarding + 5 Returning + 16 Core + 3 Safety + 4 Utility)  
👉 MVP could launch with ~20 (Onboarding + Returning + Core ID + Voting + Benefits + Security).  
  
Page contents, features and functionality  
Theme System  
Default Colors: Nigerian green & white for national identity.  
Dark Mode: Automatic (follows device) + manual toggle in settings.  
Design: Clean, accessible, with smooth transitions.  
Tech: Global theming system (React Context / Tailwind config), preferences saved locally & synced with backend.  
Scalability: Ready for seasonal/campaign themes (e.g., Independence Day).  
→ Conclusion: The theme system strengthens trust, accessibility, and brand identity while giving users personalization options.  
SplashScreen Spec  
Center: NatioID Logo + App Name (“NATIOID”)  
Background: Subtle waving Nigerian flag animation (SVG/Lottie) or gradient green-white.  
Tagline: Random from set of 4 (adds freshness, reinforces mission).  
Loader:  
Minimal animation (3 dots pulsing or thin progress bar).  
Optional text: “Initializing secure session…”  
Duration: ~2–3 seconds (auto-dismiss once initialization done).  
Transitions: Fade-in (on entry), slide/fade-out (to next screen).  
Language Selection Page  
Languages (Phase 1): English, Yoruba, Hausa, Igbo, Pidgin, Kanuri, Efik.  
UI: Large, easy-to-tap buttons with icons/flags.  
Functionality: Saves preference, applies globally, changeable later in Settings.  
Tech: i18n integration with modular packs, async loading, preference stored locally & in backend.  
Scalability: Future-ready for more languages/dialects (e.g., Tiv, Edo, Ijaw).  
→ Conclusion: The language system ensures inclusivity, accessibility, and cultural representation while staying scalable for future growth.  
👋 Welcome  
The Welcome Page is shown only to first-time users and serves as the friendly introduction to NatioID. Its purpose is to build trust, explain value, and guide users into the app.  
Key Elements:  
Headline: “Welcome to NatioID — Your Digital Identity, Simplified.”  
Description: Short text explaining core functions (secure identity management, digital voting, and access to civic services).  
Visuals: Optional illustrations or icons to make the experience engaging and guide users through first steps.  
Actions:  
Primary CTA: “Get Started” → leads into onboarding.  
Design & Experience:  
Clean, minimal, and consistent with the Nigerian green-white theme.  
Warm and approachable tone to reassure new users.  
Optimized for mobile-first readability and quick navigation.  
Onboarding Screens  
The Onboarding Screens appear only on a user’s first visit and serve to introduce NatioID in a clear, citizen-friendly way. They highlight the app’s core benefits while reinforcing trust and security as a government-backed platform.  
The flow consists of 3–4 swipeable slides, each with a short headline, description, and simple icon/visual:  
Secure Your Identity – explains safe digital ID storage.  
Access Government Services – showcases easy access to public services.  
Vote With Confidence – highlights digital voting security.  
(Optional) Trusted by Government – emphasizes official backing and data protection.  
The final slide includes a primary Call-to-Action (“Create My NatioID”)  
Design follows the green & white national theme, supports dark mode, and ensures accessibility for all citizens. This creates a professional first impression that combines citizen usability with government authority.  
📄 Registration Page  
The Registration Page allows new users to securely create a NatioID account using their official identity information.  
Purpose: Enable citizens to register with ease and confidence.  
Options for Registration:  
National Identity Number (NIN) – primary method  
Phone number or Email – inclusive alternatives  
Bank Verification Number (BVN) – optional, for added trust  
Flow: Enter ID → Validate → OTP Verification → Account Setup (PIN/Password).  
User Experience:  
Clear step-by-step process (with progress indicator)  
Simple, one-field-at-a-time form  
Help tooltips (e.g., “What is NIN?”)  
“Already have an account? Sign In” option  
Design:  
Nigerian green/white theme with clean, official layout  
Visual icons for NIN, phone, email  
Dark mode support  
Security:  
Encrypted validation via government databases  
OTP confirmation for identity proof  
Optional dual validation (NIN + BVN) for high-trust cases  
✅ This ensures nationwide accessibility (for both NIN holders and those still onboarding into the national ID system), while maintaining security and trust.  
📌 Login Page  
Overview  
The Login Page is the secure entry point into the NatioID system. It allows citizens to access their account using a PIN code or biometric authentication, with backup recovery options for security.  
  
Layout & Design  
Header Area  
App logo and Nigerian national symbol (flag/coat of arms) for trust.  
“Forgot PIN?” link positioned at the top right corner.  
Main Section  
Greeting message: “Welcome back, [Citizen’s Name]”.  
Instruction: “Enter your PIN to continue”.  
PIN input field represented by six dots (●●●●●●).  
Keypad Section  
On-screen numeric keypad (0–9).  
Delete/Backspace button.  
Biometric login button (fingerprint/face icon).  
  
Key Functions  
PIN Authentication  
Citizens enter a 6-digit PIN to log in.  
Auto-submit when all six digits are entered.  
PIN is masked for privacy.  
Biometric Authentication  
If previously enabled, fingerprint/face recognition is available.  
Uses the device’s secure biometric API.  
Forgot PIN  
Provides a recovery option via OTP (sent to registered phone or email).  
Allows reset and setup of a new PIN.  
Error Handling  
Incorrect PIN → error message with remaining attempts.  
Too many failed attempts → account temporarily locked, OTP recovery required.  
  
User Experience (UX)  
Personalized greeting with the citizen’s name.  
Large, easy-to-tap numeric buttons (mobile-first design).  
Green-white Nigerian branding for familiarity and trust.  
Accessible design with clear icons and high contrast.  
  
Security Features  
All login data transmitted via secure HTTPS/TLS.  
PINs stored in encrypted format (never in plain text).  
Biometric login handled through device-level security.  
Rate limiting and lockout prevent brute-force attempts.  
Secure session tokens issued on successful login.  
  
Scalability  
Future support for login via BVN, government email, or mobile ID.  
Multi-device login detection and notifications.  
Offline login with sync once connected.  
  
✅ This summary keeps it simple, professional, and government-grade, suitable for client documentation.  
📄 Forgot PIN Recovery Flow  
🔑 Purpose  
The Forgot PIN Recovery Flow provides a secure and user-friendly method for citizens to reset their login PIN if forgotten, ensuring continuous access to the platform while maintaining strong identity protection.  
  
🖼️ Page Flow Overview  
Identifier Input Screen  
Title: “Reset Your PIN”  
Input for NIN, registered phone number, or email.  
CTA: Send OTP  
OTP Verification Screen  
Subtitle: “Enter the 6-digit OTP sent to your registered contact.”  
OTP input (6 boxes/dots).  
Options: Resend OTP (with timer), Need Help.  
CTA: Verify  
New PIN Setup Screen  
Subtitle: “Create your new 6-digit PIN.”  
Fields: New PIN + Confirm PIN (dot-style masking).  
CTA: Save PIN  
Success Screen  
Confirmation message: “PIN successfully updated!”  
Visual: ✅ success icon + Nigeria branding (coat of arms/flag).  
CTA: Back to Login  
  
⚙️ Core Functionality  
OTP sent via SMS/email to verified contact.  
OTP validation required before PIN reset.  
Secure storage: new PIN hashed and updated in database.  
Rate-limiting and lockouts for repeated failed attempts.  
User redirected to login with updated PIN.  
  
🎨 Design & UX Notes  
Visual style consistent with login/register pages.  
PIN and OTP inputs use masked digit indicators (dots/boxes).  
Each stage includes a Back option.  
Error handling: wrong OTP, PIN mismatch, network issues.  
Friendly guidance text (“Didn’t receive OTP? Resend in 30s”).  
  
🛡️ Security Considerations  
OTP is time-limited and single-use.  
PIN stored securely (hashed + salted).  
System logs all reset attempts for audit purposes.  
Temporary lockouts for suspicious activity.  
  
🚀 Future Scalability  
Add biometric fallback (face/fingerprint reset).  
Add alternate recovery via BVN (optional).  
Multi-channel OTP delivery (SMS, Email, WhatsApp).  
  
✅ This page flow ensures ease of use for citizens while maintaining government-grade security standards.  
🔐 OTP Verification Page  
Purpose  
Confirms citizen identity during registration or PIN recovery by validating a 6-digit OTP sent via SMS or email.  
Key Features  
6-digit OTP input (auto-focus, smooth entry)  
OTP via SMS/Email, with resend option (45s cooldown)  
Change contact option if incorrect  
OTP expiry: 5 minutes; max 5 attempts before lockout  
Progress indicator (e.g., Step 2 of 4)  
User Experience  
Simple, mobile-first OTP entry boxes  
Security reassurance + fallback tips  
Works in low-connectivity environments  
Technical Considerations  
API: POST /api/verify-otp  
Secure OTP generation, expiry, and logging  
Rate limiting + attempt tracking  
Scalable to voice, WhatsApp, or authenticator apps  
Government Benefits  
Strengthens trust with secure verification  
Reduces fraud/impersonation  
Scalable nationwide for millions of citizens  
  
⚡ This keeps the documentation crisp, professional, and easy to slot into your full project docs.  
  
PIN Reset Success & Re-Login  
The PIN Reset Success Page confirms to the citizen that their login PIN has been securely updated and guides them back to the login screen.  
🔑 Key Points  
Purpose: Provide clear confirmation of a successful PIN reset and ensure secure transition back to login.  
Content:  
Success message (“Your PIN has been successfully reset”).  
Short description reassuring the user.  
CTA: “Login Now” → redirects to login page.  
Functionality:  
Old PIN is invalidated.  
Active sessions are logged out.  
Redirect to login (manual or auto after delay).  
UX:  
Simple, one-step confirmation.  
Reassuring tone, checkmark animation.  
Easy navigation back to login.  
UI/Design:  
Green/white Nigeria theme.  
Centered card with success icon + text.  
Minimal and clean.  
Tech:  
Secure PIN hashing.  
Token/session cleanup.  
Audit logging + optional SMS/Email confirmation.  
Scalability:  
Reusable for other security confirmations.  
Can extend with biometric reminders or device logout.  
  
This keeps it simple for client documentation — showing purpose, flow, design, and security in one page.  
✅ Registration Success Page   
Purpose:  
Confirms that a citizen’s NatioID account has been successfully created and guides them to the next secure step.  
Key Features:  
Success headline: “Account Created Successfully!”  
Confirmation message with reassurance.  
Success icon/animation (green checkmark).  
Primary CTA: Continue → leads to Biometric Setup or Dashboard.  
Optional CTA: Set Up Biometrics Now.  
User Experience (UX):  
Clear and celebratory confirmation.  
One main action to reduce confusion.  
Encourages biometric setup for stronger security.  
Technical Considerations:  
Confirms backend registration completion before rendering.  
Routes user based on biometric status.  
Supports offline fallback with cached confirmation.  
Scalability:  
Reusable template for other success flows (PIN reset, profile update, etc.).  
Analytics hook for tracking successful registrations.  
  
  
🔐 Biometric Setup Page   
Purpose  
The Biometric Setup Page enables citizens to activate biometric authentication (fingerprint or facial recognition) for fast and secure access to the NatioID platform.  
  
Key Features  
Automatic Detection: Checks if the device supports biometrics (Face ID/Fingerprint).  
Choice-Based Flow:  
Enable Biometrics → triggers native device biometric prompt.  
Skip for Now → user can continue using PIN/password.  
Fallback: If biometrics unsupported, app defaults to PIN/password login.  
Confirmation Feedback: On success, securely stores token and displays “Biometrics Enabled”.  
  
User Experience (UX)  
Clear & Flexible: Non-blocking option to skip setup for comfort.  
Guided Onboarding: Progress indicator shows stage in the registration flow.  
Positive Reinforcement: Visual confirmation (green checkmark animation).  
Accessibility Considerations: Clear instructions, large tap targets, and easy navigation for all device types.  
  
UI / Design  
Theme: Nigerian green-white identity theme with optional dark mode.  
Minimal & Modern: Clean layout, centered fingerprint/face illustration.  
Visual Cues: Large biometric icons, animations (e.g., fingerprint glow, checkmark success).  
Hierarchy: One main action button (Enable Biometrics) and one secondary (Skip for Now).  
  
Technical Considerations  
APIs: Uses WebAuthn / platform-native biometric APIs for broad compatibility.  
Secure Storage: Biometric preference stored locally (encrypted) and optionally linked to user account.  
Endpoint (Optional): /api/store-biometrics-preference for central logging.  
Resilience: Fallback to PIN/password if biometric fails or device not supported.  
  
Scalability  
Future-ready for:  
Multiple biometrics per account (e.g., multiple fingerprints).  
High-security actions (e.g., voting, payments) with biometric confirmation.  
Combined authentication (Biometric + PIN) for advanced security.  
  
✅ This version is professional, clean, and government-ready, balancing security, user choice, and accessibility.  
  
🏛 Citizen Dashboard (Home Page)  
1. Overview  
The Citizen Dashboard is the central landing page after registration or login. It provides citizens with a personalized overview of their identity, quick access to essential services, and timely government updates.  
The design emphasizes:  
Identity-focused – NIN, ID card, and verification always visible.  
Service-oriented – direct access to core government services.  
Dynamic & Scalable – modular widgets for future programs.  
Mobile-first – optimized for small screens, responsive across devices.  
  
2. Content Structure  
Top Section: Profile & Greeting  
Dynamic greeting (e.g., “Good morning, Abdulazeez”).  
Profile photo/avatar.  
Full name + NIN prominently displayed.  
Status badge (✅ Verified / ⚠ Pending Verification).  
ID Widget (Core Identity)  
NIN card preview (photo, name, ID number).  
Quick Actions:  
View My ID (fullscreen).  
Print ID (download/print).  
Verify Someone (scan/input NIN).  
Update Info (redirect to profile update).  
Highlights & Notifications  
System alerts (e.g., “Your ID has been verified”).  
Government programs (“Youth Grant 2025 – Apply Now”).  
Notification badges.  
Services Grid / Cards  
Voting & Elections 🗳  
Government Benefits 🎁  
Healthcare (NHIS) 🏥  
Tax & Pension 💰  
Application Services 📑  
Emergency Services 🚨  
Informational Banner / Carousel (Optional)  
Rotating banners for news, health alerts, or deadlines.  
ID Integrity Index (Optional Widget)  
Profile completeness bar (e.g., 80%).  
Encourages updates and builds a trust score.  
  
3. Functionality  
Data Integration: via APIs  
/api/user/dashboard – overview  
/api/user/id-card – ID status  
/api/notifications – alerts & updates  
Offline Support: cached ID card available offline.  
Notifications: push or polling with badge indicators.  
Expandability: modular widgets for future services.  
  
4. User Experience (UX) Principles  
Clarity: ID always visible.  
Hierarchy: Essentials at the top, services below.  
Mobile-first: one-hand scroll layout.  
Trust-oriented: badges, transparency, verification logs.  
Accessibility: large fonts, dark/light mode, tap-friendly.  
Feedback: skeleton loaders, success animations.  
  
5. User Interface (UI) Design  
Theme: Nigerian green-white palette, neutral backgrounds.  
Components: rounded cards, soft shadows, clean iconography.  
Themes: light & dark mode toggle.  
Microinteractions: smooth transitions, animated confirmations.  
  
6. Technical Notes  
Backend & APIs: REST/GraphQL with JWT auth.  
Caching & Storage: IndexedDB/SQLite for offline ID.  
Security:  
Biometric re-authentication for sensitive actions (e.g., printing ID).  
HTTPS enforced, secure token rotation.  
Performance:  
Lazy loading widgets.  
Push notifications preferred.  
  
7. Scalability & Future Growth  
Add new dashboard cards (e.g., Digital Signature, BVN sync, Education Portal).  
Expand ID Integrity Index → Citizen Trust Score.  
Promote government programs via carousel.  
Extend for admin dashboards & analytics.  
  
✅ This documentation gives developers, designers, and stakeholders a complete blueprint for the Citizen Dashboard — blending usability, trust, and scalability.  
📇 Digital ID Card (Full View)  
The Digital ID Card page serves as the secure, mobile-first digital equivalent of physical government-issued ID cards. It centralizes a citizen’s core credentials, supports offline access, and enables real-time verification. NatioID prioritizes the National Digital ID (NIN) as the default primary ID, while allowing citizens to link, view, and switch between other ID types (Driver’s License, Voter’s Card, Passport, etc.).  
  
✅ Content  
Core Identity Info: Full Name, NIN, Date of Birth, Gender, Nationality  
Additional Data: Passport Photo, Place of Birth, LGA/State of Origin, Card Issue & Expiry Date, Card Status (Active/Suspended/Expired)  
Security Elements: QR/Barcode for verification, Digital Signature (optional), Watermark/Hologram-style seal  
Multi-ID Tabs: National ID (NIN by default), Driver’s License, Voter’s Card, International Passport, Health ID, etc.  
  
⚙ Functionality  
Tap to enlarge, rotate, or view card back  
QR/Barcode generation for secure verification by authorized entities  
Copy NIN or share QR with one tap  
Offline Mode: Securely cached ID available without internet  
Save/Download card as PDF or image  
Status Indicator: Valid / Suspended / Expired  
Tab/Swipe between linked ID types  
Security toggle: Blur or hide sensitive details (NIN, DOB)  
Tap for Details: Expand into full citizen data sheet  
Optional: Biometric Match View (for linked Face/Fingerprint validation)  
  
🎯 UX Considerations  
Quick Access: Prominent shortcut from the Citizen Dashboard  
Clarity First: Name, photo, and NIN are the focal points  
Multi-ID Navigation: Swipe or dropdown to switch between ID types  
Progressive Disclosure: Show essential info by default, expand for details  
Accessibility: High contrast colors, font resize options, screen reader support  
User Trust: Display “Last Updated” timestamp for synced data  
  
🎨 UI / Design  
Card layout styled like physical ID for familiarity  
Nigerian green-white theme with subtle accents  
Light/Dark mode compatibility  
Visual authenticity: watermark, seal, or hologram background  
Large biometric/ID icons for recognition  
Minimalist, modern typography for clarity  
  
🛠 Tech Considerations  
API Endpoints:  
GET /user/id → fetch primary NIN data  
GET /user/linked-ids → fetch connected ID types  
QR Code Generation: Tokenized & time-bound for security  
Offline Storage: Encrypted localStorage / IndexedDB for cached ID  
Export Tools: PDF/image export (e.g., jspdf)  
Screenshot Protection: OS-level warning or blur (optional)  
Secure Linking: Integration with government registries for real-time validation  
  
🚀 Scalability  
Support additional ID formats (Driver’s License, Voter’s Card, Passport, Health ID)  
Plug-and-Play Integration with national databases and services  
Future enhancements:  
Biometric confirmation for high-security actions (e.g., voting, banking)  
Facial recognition match for quick verification  
NFC ID scan for advanced hardware-supported checks  
Cross-border standardization (ICAO-compliant digital ID structures)  
  
🔑 Best Flow for NatioID  
Primary Default View: Always the National Digital ID (NIN)  
Linked IDs: Displayed as secondary tabs/dropdowns for smooth switching  
Seamless UX: One “Digital ID Card” page, unified design, all IDs accessible without clutter  
  
👉 This way, the NatioID Digital ID Card page balances security, simplicity, and scalability, ensuring it works today while preparing for future government integrations.  
📄 NatioID Documentation – Digital ID Card (Full View)  
🔑 Core Purpose  
The Digital ID Card page serves as the primary identity hub for citizens. It provides secure, verifiable access to the National Identity Number (NIN) and other government-linked IDs, ensuring smooth identity validation for government, banking, healthcare, and civic services.  
  
🖼 Main Features  
1. Digital ID Display  
Default view: NIN Card (front view)  
Fields: Photo, Full Name, NIN, QR Code, Status (Valid/Expired/Suspended)  
Actions:  
Enlarge/Rotate ID  
Copy NIN  
Share QR securely  
Download as PDF/Image  
Blur/Unblur sensitive details  
  
2. Multi-ID Wallet (Swipeable Cards)  
Citizens can manage multiple IDs in one place:  
NIN (primary)  
Driver’s License  
Voter’s Card  
International Passport (read-only)  
Health ID  
Future expansion: Tax ID, Pension Card, etc.  
Navigation: Swipe left/right OR dropdown selector  
  
3. Expanded Citizen Data Sheet  
DOB, Gender, Nationality, LGA, Place of Birth  
Issue & Expiry Dates  
Linked Services (Bank KYC, Health Insurance, Voting Access)  
Last Updated timestamp for transparency  
  
4. Verification Flows  
Citizen → Show QR/NFC at banks, airports, or public offices  
Entity → Scan & Verify identity via NatioID API  
Citizen-to-Citizen Verification (scan another ID and confirm validity)  
Face Match Verification: Real-time selfie + liveness check against passport photo  
  
5. Security & Access  
Encrypted QR/NFC with time-limited tokens  
Biometric-only quick access (fingerprint/face unlock)  
Cross-device sync with secure device linking  
Offline mode: cached ID with “Last Synced on [date]”  
  
🌍 Extended Services  
Government Services Hub  
Direct access to tax, pension, welfare, and application forms (e.g., driver’s license renewal, birth certificate requests).  
e-Voting Dashboard (Future Integration)  
View elections, digital voting (where piloted), see history of votes cast.  
Complaint & Request Tracker  
Citizens can file and track requests (e.g., NIN correction, lost ID issues).  
  
🧾 Utilities & Trust Features  
Print-ready official ID (PDF/Image)  
Digital Signature Tool (sign government/legal documents)  
Multi-language support (including major Nigerian languages + voice narration for inclusivity)  
Regional personalization (show state/LGA news, local policies, upcoming civic events)  
Emergency button → sends ID + live location to police/medical services  
  
📊 Citizen Dashboard Analytics (Admin Side)  
Aggregate insights on citizen ID usage, service access frequency, and voting engagement (for government only).  
  
✅ This merged documentation balances your flows with the extra professional-grade features I suggested (face match, NFC, e-voting integration, service hub, complaints tracker, analytics).  
👤 Citizen Profile Page  
The Citizen Profile page is the personal identity hub for every registered user. It centralizes citizen data, allows controlled updates, links with other national services, and enhances trust through verification tools.  
  
✅ Content  
Profile photo (editable via face match verification for security)  
Full name  
National Identity Number (NIN)  
Date of Birth  
Gender  
Phone number (verified with OTP)  
Email address (verified with OTP)  
Residential address  
Marital status  
State of origin / LGA  
Religion (optional)  
Occupation (optional)  
Nationality (non-editable)  
Emergency contact (new addition)  
Verification status badge (Active / Pending / Suspended)  
Quick QR code for ID sharing  
  
⚙ Functionality  
View personal details in read-only mode  
Edit selected fields (phone, email, address, marital status, occupation) with OTP verification or admin approval  
Upload/change profile photo with liveness check (selfie vs stored passport photo)  
Request official data correction (redirects to form/workflow)  
Download profile data (PDF or JSON)  
Profile change history (audit log of edits, future scalability)  
Multi-device management (view and revoke active sessions)  
Logout from all devices option (extra security)  
  
🎯 UX Considerations  
Accessible from Home/Dashboard via profile icon  
Clear separation between editable vs locked fields  
Confirmation modal before saving updates  
“Why can’t I edit this?” tooltips for locked data  
Alerts for pending verification or update requests  
Support for multiple Nigerian languages + audio narration for inclusivity  
Offline snapshot (profile visible even without internet, marked with last sync time)  
  
🎨 UI/Design  
Clean card layout per section:  
Personal Info  
Contact Details  
Other Information  
Linked Services  
Circular profile photo at the top with overlay upload icon  
Colored badge for verification status (green = verified, orange = pending, red = suspended)  
Consistent green-white branding with subtle modern gradients  
Swipeable/Tab interface for Linked Services (Driver’s License, Voter’s Card, Passport, Health ID)  
  
🛠 Tech Considerations  
Secure fetch/update from Citizen Profile API (JWT or OAuth2 auth)  
OTP verification for sensitive changes (phone/email)  
Cloud-based photo upload with compression + face match AI check  
Digital signature encryption for official documents linked to the profile  
Support for caching + offline mode (critical in low-network regions)  
  
🚀 Scalability  
Security tab: PIN reset, biometric toggle, 2FA setup  
Linked Services tab: banks, NHIS, pensions, tax IDs  
Profile-based recommendations (e.g., upcoming elections, renewal reminders)  
Regional personalization (state/LGA-specific info)  
AI-based fraud detection (alert citizen if suspicious access/usage of profile occurs)  
✏️ Edit Profile Flow  
The Edit Profile flow enables citizens to safely update limited profile information while maintaining the security and integrity of national identity records. Sensitive data remains locked and can only be changed via official correction requests.  
  
✅ Editable Fields  
Phone number (requires OTP verification)  
Email address (requires OTP verification)  
Residential address (may require proof or admin approval)  
Profile photo (requires AI liveness detection)  
Emergency contact  
Occupation  
Marital status  
Religion (optional field)  
  
🔒 Non-Editable Fields  
To preserve database integrity, the following core identifiers cannot be modified directly in-app:  
NIN  
Full name  
Date of birth  
Nationality  
State of origin / LGA  
➡ These require an official correction request via NIMC or an authorized data center.  
  
⚙ Functionality  
Edit Mode  
“Edit” button activates inline editing.  
Editable fields show input boxes with pencil icons.  
Non-editable fields display a lock icon with tooltip.  
Validation & Security  
OTP required for phone/email changes.  
Profile photo changes use liveness detection + facial match.  
High-risk edits (e.g., address) may trigger moderation/approval.  
Submission Flow  
User reviews all pending edits in a confirmation modal.  
Backend validates request and logs it.  
API updates citizen record or queues for review.  
User sees success, failure, or pending approval status.  
History & Transparency  
All changes stored in Profile Change History.  
Logs include old value, new value, date/time, and approval state.  
  
🛡 Security Considerations  
OTP or biometric confirmation before saving edits.  
Audit logs for every change request.  
Suspicious activity flagged (e.g., repeated photo swaps).  
Data changes synced with NIMC backend for national record integrity.  
Optional two-step approval for sensitive fields.  
  
🎯 UX Considerations  
Inline editing for smoother user flow.  
Save/Cancel controls per section.  
Highlight unsaved changes in yellow.  
Tooltips explain why certain fields are locked.  
Loading indicator during submission.  
Accessibility: screen reader support + multilingual tooltips.  
  
🎨 UI/Design  
Pencil/edit icons for editable fields.  
Greyed-out locked fields with lock icon.  
Confirmation modal before final save.  
Green success badge / red error state after submission.  
Change history tab with status badges (Pending, Approved, Rejected).  
  
🛠 Tech Considerations  
PATCH API endpoint for partial updates.  
OTP trigger via SMS/Email service.  
Secure photo upload to encrypted storage (e.g., S3/GCS) with liveness AI.  
Local state management to handle unsaved changes.  
Rollback on failed requests.  
Database-level audit trail for compliance.  
  
🚀 Scalability & Future Enhancements  
AI-powered address validation + auto-complete.  
Integration with third-party verification services (utility bill, GPS-based proof).  
Support for document upload (e.g., proof of residence).  
Biometric confirmation (face/fingerprint unlock) for high-security edits.  
Fraud detection AI to flag abnormal update patterns.  
⚙ Settings & Security Page  
This page centralizes account preferences, security settings, and notification controls for each citizen. It reinforces trust, data protection, transparency, and personalization, ensuring users feel in control of their digital identity.  
  
✅ Content Sections  
1. 🔐 Security Settings  
Change PIN → secure PIN change flow (requires old PIN).  
Enable/Disable Biometric Login (Face/Touch ID).  
Two-Factor Authentication (2FA) toggle (future-ready).  
Set up security questions (optional backup).  
View trusted devices / active sessions with option to revoke.  
Session timeout controls (auto logout after inactivity).  
Account recovery options (update recovery phone/email).  
2. 🔔 Notifications  
Toggle SMS/Email alerts for:  
Login activity  
ID verification events  
System messages  
Push notifications for urgent government/emergency alerts.  
Channel preferences (SMS, Email, Push).  
3. 🌐 App Preferences  
Language selector (English + major Nigerian languages).  
Dark mode toggle.  
Offline mode settings (auto-cache ID for offline verification).  
Accessibility options (text size, screen reader support).  
4. 🗂 Data & Privacy  
Export personal data (PDF/JSON).  
View data access history (audit log).  
Revoke access given to third-party services (banks, hospitals, etc.).  
Profile visibility controls (public, limited, private).  
Data sharing consent management.  
5. ⚠ Account Actions  
Logout.  
Logout from all devices.  
Deactivate account (temporary).  
Delete account (requires OTP & official approval).  
  
⚙ Functionality  
Toggle switches for each setting.  
Biometric setup triggers native Face/Touch ID APIs.  
Notifications persist to backend.  
Device/session list with revoke button.  
Inline confirmation modals for destructive actions.  
Visual status indicators (e.g., “2FA Enabled ✅”).  
  
🎯 UX Considerations  
Grouped by category with collapsible sections.  
Icons (lock, fingerprint, bell, language, etc.) for clarity.  
Short explanatory text under each setting.  
Confirmation modals for sensitive actions.  
First-time setup wizard (PIN + biometrics encouraged).  
  
🎨 UI/Design  
Consistent with NatioID theme (green/white + neutrals).  
Lucide or Material icons for familiarity.  
Feedback banners for success/failure.  
Red warning modals for irreversible actions (delete account).  
Green success banners for saved preferences.  
  
🛠 Tech Considerations  
Endpoints:  
GET/POST for user settings  
PATCH for updates (PIN, biometrics, notifications)  
DELETE for device sessions  
Security:  
PIN hashed (bcrypt/scrypt).  
Biometrics stored in Secure Enclave/Keychain (never sent to backend).  
JWT-based session management.  
Compatibility:  
Fallback for older devices (PIN instead of biometrics).  
Audit: Logs of every setting update kept for accountability.  
  
🚀 Scalability & Future Enhancements  
Passcode lock for entering settings.  
Biometric-only access (skip PIN).  
Adaptive security: auto-prompt for 2FA if login from new device/location.  
Federated login for institutions (universities, hospitals, banks).  
Privacy tiers (Public / Limited / Private).  
AI-driven fraud/suspicious login alerts.  
Integration with national emergency broadcast system for urgent push alerts.  
🛡 Verification Center  
This module provides citizens with a secure, auditable history of all verification events involving their NatioID (NIN). It ensures transparency, accountability, and citizen control over where and how their identity is used.  
  
✅ Content  
Verification Logs (Table/List/Timeline):  
Date & time  
Entity name (e.g., INEC, GTBank, Lagos General Hospital)  
Purpose (ID check, voter registration, KYC, hospital access, employer verification)  
Location (if available, GPS/IP)  
Status: ✅ Success / ❌ Failed / ⏳ Pending  
Search & Filters:  
By date range  
By institution type (government, bank, hospital, employer)  
By status (success, failed, pending)  
Detail View (Tap/Expand):  
Metadata about the verification (channel, method, device/IP if applicable)  
Fields scanned (e.g., NIN, QR code, DOB, biometrics)  
Consent record (Yes/No, timestamp)  
Option to report suspicious activity  
  
⚙ Functionality  
Paginated or infinite scroll log  
Pull-to-refresh for latest updates  
Tap/click a record → expands into detailed view  
Backend API with filtering & pagination  
Export options: Download history as PDF/CSV, or send via email  
Alerts: Notify citizen instantly for failed/unknown verification attempts  
Flagging system: Citizen can raise a dispute on suspicious entries  
  
🎯 UX Considerations  
Bank-statement style clarity (trustworthy look & feel)  
Logs sorted by most recent first  
Institution logos/icons for quick recognition  
Color-coded statuses (green = success, red = failed, orange = pending)  
Highlight failed or unauthorized attempts at the top with alert banner  
Empty state illustration if no verifications yet  
  
🎨 UI/Design  
Neutral + green palette (trust, national identity brand)  
Card-based or vertical timeline layout  
Shield/check/error icons for statuses  
Modal popup or sliding drawer for event details  
Export/download button always visible (top-right)  
  
🛠 Tech Considerations  
API Endpoints:  
GET /verifications → Fetch paginated list  
GET /verifications/:id → Single verification details  
POST /verifications/report → Report suspicious activity  
Security & Privacy:  
Logs encrypted at rest & in transit  
Immutable audit trail (cannot be altered or deleted)  
Access requires biometric/PIN confirmation  
Rate limiting to prevent scraping or brute force attempts  
Logs only visible to authenticated citizen  
Notifications:  
Optional push/SMS/email when a new verification is logged  
  
🚀 Scalability & Future Enhancements  
Real-time approval flow (Strict Mode): Citizen must approve before ID can be verified by third parties  
AI anomaly detection: Flag unusual access patterns or high-risk attempts  
Geo-mapping view: Display verification activity on a map  
Institution reputation scoring: Track frequency of failed attempts from organizations  
Integration with fraud monitoring dashboards for admins  
  
🔑 Impact: The Verification Center empowers citizens with visibility, control, and peace of mind, ensuring NatioID is transparent, auditable, and fraud-resistant.  
🔗 Linked Services Page  
Where citizens can view, connect, and manage all government and private services tied to their digital identity. Provides full transparency, granular consent, and security control over data-sharing.  
  
🔗 Summary  
The Linked Services page centralizes all integrations (banks, healthcare, education, telecoms, electoral bodies, etc.) that use NatioID for verification, KYC, or digital identity authentication. Citizens can:  
Review existing connections  
Control what data is shared  
Revoke access instantly  
Connect new services securely  
  
✅ Content  
List of Linked Services (with logos/icons):  
Government: INEC (Voter Register), FRSC (Driver’s License), NIMC (NIN), NHIS (Health), JAMB, Tax Office  
Finance: GTBank, Access, Paystack, Mobile Money  
Healthcare: Hospitals, HMOs, Insurance  
Telecom & Utilities: MTN, GLO, PHCN, Water Board  
Education & Employment: Universities, NYSC, Employers  
Key Service Info Shown:  
Service name + logo  
Status → Verified / Pending / Failed  
Data shared → NIN, DOB, contact info, biometrics (if any)  
Last sync / activity date  
Actions:  
Connect New Service button  
Revoke Access / Refresh for each  
  
⚙ Functionality  
Service Details View:  
Date linked  
Data fields shared  
Last sync status  
Service’s privacy notice link  
Revoke / Refresh button  
Connect New Service Flow:  
Citizen starts consent-based OAuth/API handshake  
Chooses which data fields to share  
Confirmation + success/failure status  
Background Sync:  
Auto-updates linked service data periodically  
Alerts for sync failures  
Audit Logs:  
Record of all link/unlink actions  
Notifications for unusual activity  
  
🎯 UX Considerations  
Categorized sections → Government | Finance | Health | Education | Utilities  
Trust indicators: Official logos + verified badges for approved institutions  
Warnings before revoking critical services (e.g., voting eligibility, SIM registration)  
Color/status cues:  
✅ Linked  
🕓 Pending  
⚠ Failed/Error  
Empty state illustration → Encourage connecting first service  
  
🎨 UI / Design  
Card layout (service logo, status, last activity)  
Tab or filter option → browse by category  
Nigeria-inspired palette (green + neutral backgrounds)  
Toggle switches for permissions  
Modal confirmation screens for linking/revoking  
  
🛠 Tech Considerations  
API Endpoints:  
GET /linked-services → fetch all services  
POST /link-service → start new connection  
PATCH /linked-service/:id → update permissions / refresh  
DELETE /linked-service/:id → revoke access  
Security:  
End-to-end encrypted consent flows  
Revoke = instant invalidation of tokens/keys  
Immutable logs of all service interactions  
Data minimization (only necessary fields shared)  
Offline Resilience:  
If service API is down → show fallback message, retry queue  
  
🚀 Scalability & Future Enhancements  
Upcoming integrations: International Passports, Pension & Tax data, Digital Health Records  
One-click “Connect All” for bundled services (e.g., all banks)  
Notifications when a new service links to your ID  
Analytics dashboard → See service usage trends  
Marketplace of services → Citizens browse & connect new official integrations  
Universal Login (SSO): Use NatioID to sign in securely across apps/websites  
  
🔑 Impact  
The Linked Services hub transforms NatioID into a secure national identity gateway. Citizens gain transparency, ownership, and control over how their data is used, while institutions benefit from trusted, standardized identity verification.  
🗳 Voting Page  
The Voting Page empowers citizens to participate in Presidential and Governorship elections, with secure digital infrastructure, candidate transparency, and real-time result monitoring.  
It combines eligibility checks, candidate education, encrypted vote casting, and live result displays — designed for trust, accessibility, and national-scale scalability.  
  
✅ Content  
Election Types: Tabs or dropdown for Presidential | Governorship  
Upcoming Elections: Position, date, constituency, status  
Eligibility Card: Verified via NIN, age, and location (e.g., “Eligible – Lagos State Governorship Election”)  
Candidate Profiles:  
Photo & Party Logo  
About (short bio + image)  
Achievements (bullet points)  
Campaign Promises / Aims  
Expandable profile (full manifesto, videos, interviews)  
Voting Section: “Cast Vote” button (enabled during official window only)  
Voting History: Secure log of past participation (date, type, success/fail)  
Live Results Dashboard: Graphs/bar charts showing real-time tallies (with disclaimer: “Provisional results – subject to INEC verification”)  
Voter Education: Step-by-step guide, FAQs, best practices for secure digital voting  
Feedback / Report Issues: Form to flag irregularities or technical problems  
  
⚙ Functionality  
Eligibility Verification: Real-time validation (NIN, residency, age)  
Secure Vote Casting:  
Multi-step wizard (select candidate → confirm → authenticate → submit)  
PIN + biometric (face/fingerprint) before final submission  
Encrypted vote storage with timestamp  
Candidate Interaction: Tap card → expanded profile with manifesto  
Live Results: Updates pulled from electoral servers at intervals (push or pull mode)  
Audit Trail: Blockchain-backed immutable record (non-identifiable, for transparency)  
Notifications: Election reminders, “Voting is now open”, live results updates  
Offline Support: Cache candidate info, show last synced live results  
Fraud Protection:  
One vote per user (backend lock)  
Device fingerprinting (prevent duplicate votes across devices)  
Session expiry & time-limited tokens  
  
🎯 UX Considerations  
Clear split between Presidential and Governorship elections  
Prominent “Am I eligible?” section with green check or red warning  
Candidate cards designed for quick comparison, expandable for details  
Voting flow kept simple: Select → Confirm → Authenticate → Submit  
Visual focus during vote (darkened background, single-choice UI)  
Accessibility:  
Multi-language (English, Hausa, Yoruba, Igbo, Pidgin)  
Text-to-speech for candidate bios and instructions  
Large buttons and contrast-friendly design  
  
🎨 UI/Design  
Neutral & official look (trust-focused)  
Tabs or segmented control for Election Types  
Candidate cards with party colors/logos  
Live results displayed as charts (bar, pie, percentage)  
Green ✅ = Eligible, Red ❌ = Not Eligible, Yellow ⚠ = Pending verification  
Nigeria color palette (green-white) with neutral grays for balance  
  
🛠 Tech Considerations  
APIs: /elections, /candidates, /cast-vote, /results  
Security:  
AES-256 encryption + blockchain audit log  
Biometric + PIN authentication  
Backend vote uniqueness validation  
Scalability:  
High-availability clusters during elections  
Load balancing for live result dashboards  
Transparency: Provisional data labeled clearly until final INEC confirmation  
Notifications: Push service for reminders and live updates  
  
🚀 Scalability  
Extendable to Local Council, Referendums, Diaspora Voting  
Candidate profiles can embed campaign videos, manifestos, social feeds  
Live debates or Q&A integration (future feature)  
AI-powered fraud detection (e.g., flagging unusual voting patterns)  
Real-time national turnout dashboards for citizens and observers  
  
✅ Final Note:  
The Voting Page in NatioID is not just a digital ballot box but a transparent election hub — informing citizens about candidates, ensuring secure voting, providing live results, and maintaining trust through audit trails and inclusive design.  
🆘 Help & Support Center  
📌 Purpose  
Provide citizens with a centralized hub for guidance, troubleshooting, and reporting issues. This page reduces user frustration, improves accessibility, and builds trust by offering self-service tools, human support escalation, and emergency resources.  
  
✅ Content  
FAQs categorized by topics:  
Registration  
Voting  
Security & Privacy  
Account Recovery  
Linked Services  
Technical Issues  
Issue Reporting Form:  
Categories: Login issues, verification errors, suspicious activity, general inquiries  
Option to attach screenshots/evidence  
Chatbot (AI or scripted):  
Instant answers for common questions  
Escalates to human agent if unresolved  
Contact Options:  
Phone, Email, Live Chat, Social Media links  
Emergency Support Section:  
Direct numbers for Police 🚓, Medical 🚑, Fire 🚒  
  
⚙ Functionality  
Searchable FAQs with autocomplete  
Submit & track support tickets (with ticket ID + status tracking)  
Chatbot integration with fallback → human support → ticket creation  
Multi-channel contact routing: Email, SMS, WhatsApp, Call Center  
Push/email notifications for support responses  
Multi-language support  
  
🎯 UX Considerations  
Intuitive layout → Quick access to popular FAQs  
Clear step-by-step flow for issue reporting  
Mobile-first responsive design with collapsible FAQ sections  
Language toggle for accessibility  
Emergency support always pinned/visible  
Feedback option: “Did this solve your problem? 👍👎”  
  
🎨 UI/Design  
Consistent green-white NatioID theme  
Clear icons for support methods: ☎️ Phone, ✉️ Email, 💬 Chat  
Success modal after ticket submission  
Ticket progress bar: Pending → In Progress → Resolved  
Accordion layout for FAQs (expand/collapse)  
Emergency contacts highlighted in red alert-style cards  
  
🛠 Tech Considerations  
Backend Ticket Management (CRM integration)  
Chatbot Platforms: Google Dialogflow / Microsoft Bot Framework / Rasa  
Notification system for ticket updates (Push + Email)  
Knowledge base API for FAQs (auto-updatable)  
File upload support for attachments in issue reporting  
Analytics for top FAQs, response times, ticket resolution rate  
  
📈 Scalability  
Live video support or callback features  
AI-powered smart suggestions for self-help  
Integration with voice assistants (Google Assistant, Alexa)  
Expansion to regional/local support centers  
AI monitoring for detecting repeated unresolved issues  
  
✅ Final Summary  
The Help & Support Center provides FAQs, chatbot, issue reporting, human escalation, multi-channel contact, and emergency numbers — ensuring users always have access to guidance and support. With automation, CRM integration, and AI-powered suggestions, it balances self-service efficiency with human reliability, scaling with user growth and national adoption.  
  
📜 Activity Log / Audit Trail  
✅ Content  
Timeline of user activities: logins, profile updates, vote cast, PIN changes, linked services access.  
Metadata: Date, time, device, location (IP or GPS where possible).  
Option to filter by activity type/date.  
Admin-side audit trail: approvals, edits, resets, and backend security events.  
⚙ Functionality  
Secure, tamper-proof log storage.  
Real-time syncing across devices.  
Alerts & notifications on suspicious activity.  
Export logs (PDF/CSV) for audits or legal verification.  
Blockchain-backed logging (optional) for immutability.  
“Report suspicious activity” button for users.  
🎯 UX  
Simple timeline or table view.  
Highlight critical security events in red (e.g., failed logins).  
One-tap action to dispute or confirm an activity.  
Filter & search for easy navigation.  
🎨 UI  
Clear timestamps with icons (🔑 login, 📝 profile edit, 🗳 voting, 🔗 linked service).  
Vertical scrollable timeline with date headers.  
Mobile-friendly design with swipe filters.  
🛠 Tech  
Encrypted log storage (AES + server-side integrity checks).  
Blockchain option for government-level immutability.  
Real-time log syncing APIs.  
Integration with security monitoring tools (SIEM, intrusion detection).  
📈 Scalability  
Expand logs to cover third-party integrations (banks, hospitals, telecoms).  
Admin dashboard for nationwide monitoring & analytics.  
AI-powered anomaly detection (flag unusual user behavior).  
📄 Digital Consent / Terms Page  
🔹 Purpose  
The Digital Consent / Terms Page ensures every user explicitly agrees to the legal, privacy, and data-sharing conditions before using NatioID services. This page is a compliance-critical checkpoint that establishes trust, protects the government legally, and safeguards citizen rights in line with NDPR, GDPR, and global digital ID standards.  
  
🧾 Page Content  
Title: “Terms & Conditions & Digital Consent”  
Sections (Expandable/Tabbed):  
Terms of Service (rules, usage, obligations)  
Privacy Policy (data handling, security measures)  
Data Collection & Sharing Disclosure (who has access + why)  
Biometric Usage Consent (fingerprint/face data usage and protection)  
Government Access Permission (lawful access by security or agencies)  
Actions:  
✅ Checkbox: “I have read and agree to the Terms & Conditions.”  
🔘 Continue button (disabled until checkbox is ticked & page scrolled).  
📥 Optional link: “Download full document (PDF).”  
  
⚙ Core Functionality  
Dynamic Content:  
Terms pulled from backend API or CMS → allows future updates without app changes.  
Cached copy for offline fallback.  
Consent Flow:  
User must scroll (optional UX pattern to encourage reading).  
Continue button only activates when consent is given.  
Rejecting consent → user cannot proceed.  
Storage:  
Acceptance logged locally + server-side with:  
{  
 "user\_id": "12345",  
 "accepted\_at": "2025-09-01T15:30:00Z",  
 "terms\_version": "v1.2",  
 "privacy\_version": "v1.2",  
 "language": "en"  
}  
Multi-Language Support:  
Auto-loads language from user profile (English, Hausa, Yoruba, Igbo, Pidgin).  
Future-ready for French/Arabic for ECOWAS use.  
Offline Handling:  
If terms were previously cached → allow consent offline, sync acceptance later.  
  
🎯 UX Considerations  
Split long legal text into accordion sections or tabs.  
Highlight key clauses (biometrics, government access, responsibilities).  
Clear, friendly explanation why consent is needed (security, legal compliance, user protection).  
Designed for small screens → responsive, scrollable, touch-friendly.  
  
🎨 UI / Design  
Theme: Green-white national identity branding.  
Icons per section:  
📑 Terms → document icon  
🔒 Privacy → lock/shield  
🧬 Biometric → fingerprint/face  
🛡 Government → badge/shield  
Layout:  
Title → Sections → Checkbox → Footer Buttons  
Sticky footer with “Back” | “Accept & Continue”  
  
🛠 Technical Requirements  
Frontend:  
Accordion components, checkbox gating, multilingual rendering.  
Disabled Continue until consent given.  
Backend:  
API /api/consent/accept with POST payload of consent metadata.  
Store version history for each user → prompt re-consent if updated.  
Security:  
Consent entries digitally signed (hash of user\_id + timestamp).  
Immutable logging (optionally blockchain-based for audit).  
Reject attempts logged.  
  
🚀 Scalability & Compliance  
Version Control: Users prompted to re-consent when terms update.  
Multi-Region Support: Adaptable to NDPR (Nigeria), GDPR (EU), HIPAA (health).  
Revoke Consent: Available in Settings → disables certain features (e.g., no biometrics if consent revoked).  
Legal Proof: Consent receipts exportable as PDF.  
  
✅ Final Summary  
The Digital Consent / Terms Page is a trust and compliance cornerstone for NatioID. It guarantees that users are fully aware of how their data, biometrics, and digital ID will be managed. Through dynamic document loading, secure acceptance tracking, multilingual accessibility, and scalable compliance features, it balances legal obligations, user transparency, and a smooth onboarding experience.  
  
📢 Complaint Tracking Page  
📝 Purpose  
The Complaint Tracking Page empowers citizens to submit complaints (lost ID, incorrect info, fraud, app issues, etc.) and monitor resolution progress. It promotes transparency, accountability, and trust in the civic process by giving users visibility into how their issues are handled.  
  
✅ Page Content  
Complaint ID (auto-generated, shown after submission).  
Complaint Type (dropdown): Lost ID, Wrong Data, App Issue, Fraud Report, Access Denied, Others.  
Description (detailed text area with tooltips/examples).  
Attach File/Image (optional proof: screenshot, document, PDF).  
Submission Date (auto-filled).  
Status: 🟡 Pending → 🔵 In Review → ✅ Resolved → 🔴 Rejected.  
Response from Authority: optional admin message or resolution note.  
History Log: timeline from submission → review → updates → closure.  
  
⚙ Core Functionality  
📤 Submit new complaint via form.  
🔍 Track complaint in real-time with Complaint ID.  
📜 View past complaints (for logged-in users).  
🔔 Notifications when status changes.  
📎 Upload attachments (images, PDFs, documents).  
🕵 Anonymous reporting option (for fraud/tip-offs).  
⚡ Auto-routing to correct agency via backend rules.  
📑 Export complaint + resolution as PDF (optional).  
  
🎯 UX Considerations  
Clear progress tracker (stepper UI with icons).  
Mobile-first, responsive form.  
Quick lookup with Complaint ID.  
Estimated resolution time displayed if available.  
Tabbed interface: “➕ New Complaint” | “📂 My Complaints”.  
Status Color Codes:  
🟡 Pending  
🔵 In Review  
✅ Resolved  
🔴 Rejected  
Tone: friendly yet formal, accessible language.  
  
🎨 UI / Design  
Theme: Green & White (Nigeria) with neutral greys.  
Form Layout: simple, guided, icons for complaint type.  
Tracker: progress bar / parcel-tracking style.  
Tabs:  
New Complaint: form with dropdown + upload.  
My Complaints: list + filter by type/status/date.  
Accessibility: text labels + icons + color codes.  
  
🛠 Technical Requirements  
Frontend:  
Complaint form with validation.  
Complaint tracker + status visualization.  
Complaint history (login required).  
Backend / API:  
/api/complaints/submit (POST).  
/api/complaints/status/:id (GET).  
/api/complaints/user/:id (GET).  
Database:  
complaints (  
 complaint\_id VARCHAR(20) PRIMARY KEY,  
 user\_id VARCHAR(20),  
 type VARCHAR(50),  
 description TEXT,  
 attachment\_url VARCHAR(255),  
 status ENUM('pending','review','progress','resolved','rejected'),  
 response TEXT,  
 created\_at TIMESTAMP,  
 updated\_at TIMESTAMP  
)  
  
complaint\_updates (  
 update\_id INT AUTO\_INCREMENT PRIMARY KEY,  
 complaint\_id VARCHAR(20),  
 status VARCHAR(20),  
 note TEXT,  
 updated\_by VARCHAR(20),  
 updated\_at TIMESTAMP  
)  
File uploads: secure storage with size/type limits.  
Notifications: email/SMS/push on updates.  
Role-based access: Admins update statuses, add notes, close complaints.  
  
🚀 Scalability & Future Enhancements  
Filtering (by type, status, date).  
Complaint trend analytics (frequent issues, resolution times).  
Escalation rules (auto-flag overdue complaints).  
Multi-language support.  
Feedback option after resolution (citizen satisfaction).  
Integration with CRM/ticketing systems.  
  
✅ Final Summary  
The Complaint Tracking Page is a centralized, transparent, and user-friendly module where citizens can report, track, and resolve identity-related issues. With features like real-time tracking, notifications, history logs, file uploads, and admin audit controls, it ensures efficient resolution and strengthens citizen trust in the NatioID system.  
Tutorials & Coach Marks  
  
🎯 Purpose  
The Tutorials & Coach Marks system guides first-time users (and returning users after major updates) on how to use NatioID securely and effectively. It improves adoption, reduces errors, supports digital literacy, and builds trust in the digital identity platform.  
  
✅ Content  
Intro Guide (modal/overlay) — triggered on first app use or after updates.  
Coach Marks (spotlight highlights) for core features:  
Language selection  
Digital ID viewing  
Voting  
Profile & settings  
QR scanning  
Full Tutorial Library — optional standalone page with:  
Short guides or videos  
How-to articles (e.g., “Reset your PIN”, “Report lost ID”)  
Emergency Quick Guide (lost/stolen ID reporting)  
Contextual Help Pop-ups — appear when a user accesses a feature for the first time.  
Illustrations / Demo Animations (Lottie or video).  
Search & filter bar (by feature/topic).  
“Try It Yourself” Interactions — safe practice flows (e.g., mock voting).  
  
⚙ Functionality  
Show on first use or “What’s New” after major updates.  
Option to replay tutorials anytime (via Help/Settings).  
Language toggle for tutorials.  
Accessibility features: audio narration, captions, high-contrast support.  
Progress tracking — e.g., “3 of 5 steps completed”.  
Skip / Don’t show again option.  
Version-aware walkthroughs — highlight new features only.  
Deep Links — tutorials can jump directly to the related feature.  
Adaptive tutorials — adjust based on user’s experience level.  
  
🎯 UX Considerations  
Simple, friendly microcopy (localized and easy to read).  
Step-by-step onboarding flow (not overwhelming).  
Gamified progress — badges or completion rewards.  
Undo / Replay per step for clarity.  
Role-based flows (Citizen, Official, Admin).  
Responsive, touch-friendly design.  
Smart triggers — tutorials suggested if user seems stuck (e.g., failed login → “Reset PIN” guide).  
  
🎨 UI / Design  
Light overlay + spotlight effect for coach marks.  
Speech bubbles / arrows pointing to UI elements.  
Visual consistency with NatioID theme (green-white, Nigerian identity).  
Highlight colors — subtle green glow to match branding.  
Icons for tutorial categories.  
Optional animated mascot/guide (e.g., stylized eagle or handshake icon).  
Dark mode & high-contrast themes supported.  
Navigation controls: Previous, Next, Done.  
  
🛠 Tech Considerations  
Store tutorial completion state in localStorage or via backend flag for persistence across devices.  
Tutorials configurable via CMS or JSON — easy to update without redeploy.  
Cache tutorials offline for low-connectivity areas.  
Analytics tracking — monitor completion/drop-off points.  
Multilingual support (English, Hausa, Yoruba, Igbo, etc.).  
Support for Lottie animations and embedded videos.  
  
🚀 Scalability  
Add tutorials per user role (Citizen, Admin, Official).  
Trigger based on user behavior (e.g., hasn’t scanned QR yet).  
A/B testing — test different tutorial flows for retention.  
AI-driven assistant — suggest relevant guides contextually.  
Community-driven tutorials — verified tips from other users.  
  
🏆 Final Summary  
The Tutorials & Coach Marks system in NatioID provides a guided, interactive learning experience for users of all literacy levels. With onboarding flows, contextual help, gamified progress, and multilingual support, it ensures users quickly learn core features while maintaining trust and accessibility. Scalable by role and behavior, it evolves into a dynamic learning hub that supports both citizens and officials in Nigeria’s digital identity ecosystem.  
⚠ Safety & Security  
Security is the backbone of NatioID. This section provides tools for emergency response, account protection, and resilience in low-connectivity environments, ensuring citizens always feel safe and in control of their digital identity.  
  
4.1 Security Alerts / SOS 🚨  
📌 Purpose  
Provide citizens with an instant way to alert authorities or trusted contacts in emergency situations such as ID theft, coercion, impersonation, or physical danger.  
✅ Features  
SOS Trigger  
Long-press button, triple-tap gesture, or shake phone.  
Option for a discreet trigger (hidden button).  
Alert Recipients  
Pre-defined emergency contacts.  
Local law enforcement / National ID Control Center.  
Option for anonymous fraud report.  
Location Sharing (GPS when online, cell-tower SMS fallback offline).  
Emergency Signals (optional siren sound or flash for distraction).  
Silent Countdown before sending (e.g., “Sending alert in 5s… Cancel”).  
Fraud Reporting: Report suspicious use of your NatioID (impersonation, duplicate ID).  
🛠 Tech  
GPS & SMS/Email APIs.  
Encrypted alert logs.  
Push notifications to police dashboard.  
Biometric re-authentication for cancellation (prevent abuse).  
🔐 UX  
Always accessible (even from lock screen).  
Hold-to-trigger to reduce false alarms.  
Clear feedback: “Alert sent successfully”.  
Offline fallback (SMS or cached alert).  
  
4.2 Security Center 🔒  
📌 Purpose  
Centralized hub for all security-related settings and monitoring.  
✅ Features  
PIN / Biometric Management  
Change PIN, enable Face ID / fingerprint.  
Device & Session Management  
View active devices and logins.  
End unknown sessions remotely.  
Security Notifications  
Alerts for login attempts, PIN changes, profile edits.  
2FA & Trusted Devices (future roadmap).  
Liveness Re-verification  
Periodic re-check with facial scan to avoid ID spoofing.  
Fraud Alerts Dashboard  
Flag suspicious activity (duplicate logins, multiple failed attempts).  
🛠 Tech  
Secure session validation on backend.  
Push notifications (FCM, OneSignal).  
JWT / Refresh token rotation.  
Integration with national fraud-detection systems.  
🔐 UX  
Easy toggles for non-technical users.  
Traffic-light indicators for “Security Strength”.  
Accessible via Profile → Security Center.  
Educational tooltips (e.g., “Why enable 2FA?”).  
  
4.3 Offline Mode 📶  
📌 Purpose  
Guarantee core identity access and verification even without internet — critical in rural or under-connected areas of Nigeria.  
✅ Features  
Offline Digital ID Card  
Securely cached on device.  
QR Code available for offline scanning.  
Cached Profile Info  
Last-synced citizen details available.  
Offline Verification  
Peer-to-peer verification via QR scan.  
Emergency SOS via SMS (if no data).  
Future Roadmap: Offline vote casting → sync when online.  
🛠 Tech  
Encrypted local storage (SQLite / IndexedDB).  
Service Workers for PWA offline support.  
QR Codes with expiry timestamp for fraud prevention.  
Background sync on reconnect.  
🔐 UX  
Banner: “You are offline”.  
Last-updated timestamp visible.  
Warning if cached data is expired.  
Offline ID watermark (to prevent screenshots being reused indefinitely).  
  
✅ Final Notes  
All security actions are audit-logged in Activity Timeline (Section 28).  
Zero-trust design: always verify before critical actions.  
Accessibility: large buttons, voice prompts, haptic feedback.  
Future integration with NIMC & Nigerian Police emergency systems.  
📷 Scan ID Page – QR/Barcode Scanner  
1. Purpose  
The Scan ID page allows citizens, agents, and officials to securely scan QR or Barcode embedded on NatioID cards for instant identity verification. It ensures trust, prevents fraud, and supports both individual and institutional verification use cases.  
  
2. Features  
Content  
Live camera feed (scanner) with alignment frame  
Instruction text: “Align the QR/Barcode within the frame”  
Flashlight toggle (low-light support)  
Manual entry fallback (NIN or ID number)  
Verification Result (post-scan):  
Verified full name  
Photo  
ID type & number (e.g., NIN, Voter ID)  
Verification status (✓ Verified / ⚠ Invalid / ❌ Not found)  
ID validity/expiry date  
Timestamp  
Optional action buttons: Report ID / Flag suspicious ID  
  
3. Functionality  
Real-time scanning using device camera (auto-focus, scanning frame)  
Secure call to backend verification API (end-to-end encrypted)  
Encrypted QR payload with:  
Digital signature (JWT)  
Expiry timestamp (prevents reuse)  
Role-based access:  
Citizens → Basic info only  
Agents/Officials → Extended verification details  
Offline fallback (cached verification + local signature validation)  
History of past scans (optional, for admin/agents)  
Error handling for invalid, expired, or tampered codes  
Accessibility support: audio + haptic feedback  
  
4. UX Considerations  
Fast, seamless scanning (show spinner while verifying)  
Clear guidance (visual + text)  
Large, high-contrast buttons for accessibility  
Manual override option when scan fails  
Minimal, distraction-free interface  
Low-light optimization and mobile-first design  
  
5. UI/Design  
Centered scan frame with transparent overlay  
Optional animated scan line  
Verification result colors:  
✅ Green = Verified  
⚠ Yellow = Suspicious/Warning  
❌ Red = Invalid  
Official verification watermark/seal (for agent view)  
Light/Dark mode support  
  
6. Technical Considerations  
Camera access APIs:  
Web: getUserMedia()  
Mobile: native modules (Android/iOS)  
QR/Barcode decoding libraries: jsQR, ZXing, react-native-camera, ZBar  
Encrypted payload validation (JWT with server’s public key)  
Secure API with audit logging (every verification recorded)  
Permission handling for camera, storage, offline mode  
  
7. Scalability  
Batch scanning mode (for polling stations, border checks)  
NFC and biometric verification support in future  
Verifiable Credentials (DID, W3C standard) for global compatibility  
API integration for banks, schools, hospitals, and government services  
Centralized admin dashboard to monitor verification activity  
  
8. User Flow  
Home/Dashboard → Scan ID → Verification Result → Optional Actions (Flag / Report / Save / Batch Verify)  
🖨 Print ID Page – Generate/Download Printable ID  
This page allows citizens to securely generate a printable version of their digital identity card(s) (e.g., NIN, Voter ID, Driver’s License). It ensures access to official identity in offline or emergency use, with formats suitable for both personal print and official agency issuance.  
  
✅ Content  
Preview of digital ID card(s): front and optional back view  
Clear action buttons:  
Download as PDF  
Download as Image (JPEG/PNG)  
Print directly  
Instructional text:  
“Use only for official purposes. Always keep your digital copy updated.”  
“Not valid if tampered” (seal/watermark disclaimer)  
Optional: Signature placeholder / stamp space  
System-generated metadata: issuance date, expiry date, ID type  
  
⚙ Functionality  
Render ID in high-resolution, print-friendly format  
Export options:  
PDF (A4 sheet or PVC-ready card size)  
Image (JPEG/PNG for mobile storage)  
Support both portrait and landscape orientation  
Ensure QR code remains scannable for verification  
Prevent printing of expired or incomplete IDs  
Server-side: embed digital watermark & anti-forgery hash  
Role-based permissions:  
Citizen → only their own IDs  
Admin/Agency → batch printing for issuance  
  
🎯 UX Considerations  
Simple, minimal interface with ID preview in center  
Options for multiple IDs (if citizen has more than one)  
Confirmation before final print/download  
Accessibility: large readable text, color contrast, tooltips  
Mobile-friendly: “Save to device” and share options (email/WhatsApp)  
Tooltip: “Keep your printed ID in a safe place. Do not share publicly.”  
  
🎨 UI/Design  
Professional look with green-white Nigerian theme  
ID card design mimics real physical NIN/Voter’s ID with authenticity  
Background watermark (Coat of Arms, agency seal)  
Optional light/dark print themes  
Consistent typography, borders, spacing for formal appearance  
ID preview card in center → actions below  
  
🛠 Technical Considerations  
Frontend libraries:  
react-to-print, html2canvas, jspdf, or pdf-lib  
Backend libraries:  
Node/Django: pdfkit, wkhtmltopdf  
PHP: TCPDF, DomPDF  
ID generation should use SVG/Canvas for sharp scaling  
Secure handling: auto-delete temporary files after generation  
Embed QR code verification link tied to backend verification system  
Log every print/download event in Audit Trail  
  
🚀 Scalability  
Branding for agencies (NIMC, INEC, FRSC, etc.) per ID type  
Batch printing for official centers/agents  
Integration with PVC card printers (future expansion)  
Version tracking: each printed copy has unique hash/serial  
Possible NFC-enabled smart card support (future upgrade)  
  
🔄 Suggested Flow  
Citizen Dashboard → View Digital ID → Options → Print ID → Preview → Download (PDF/Image) or Print → Confirmation → Audit log entry  
🚨 Report Lost/Stolen/Compromised ID Page  
This page allows citizens to report their identity card(s) as lost, stolen, or compromised, triggering immediate flagging, optional deactivation, and notifications to relevant authorities. It ensures security for the citizen while reducing the risk of fraudulent use.  
  
✅ Content  
Heading: “Report Lost, Stolen, or Compromised ID”  
Explanation:  
“If your ID has been lost, stolen, or misused, report it immediately to protect your identity and prevent misuse.”  
Select affected ID type(s):  
National ID (NIN)  
Voter’s Card  
Driver’s License  
Passport  
Others (Custom input)  
Reason for report (dropdown):  
Lost  
Stolen  
Compromised (unauthorized use, fraud)  
Optional fields:  
Date & place of loss/theft  
Brief description or comment  
Upload supporting document (police report, affidavit – PDF/JPG)  
Emergency contact toggle: Auto-notify “ICE” contact (In Case of Emergency)  
CTA Button: “Report Now”  
  
⚙ Functionality  
Instantly flag reported ID(s) in backend system  
Auto-disable digital QR/Barcode linked to ID (temporary until replacement)  
Notify relevant government agency (NIMC, Police, INEC, Immigration, etc.)  
Generate unique tracking reference number for the report  
Confirmation via Email/SMS sent to user  
Option to reverse the report (with strict verification like OTP/biometrics)  
Auto-log entry in Activity Timeline & Security Center  
Admin dashboard: view, verify, and process reports  
  
🎯 UX Considerations  
Urgent tone with clear red warnings:  
“Once reported, this ID cannot be used until reviewed or reissued.”  
Accessible button from Profile & Security Center  
Step-by-step wizard flow for clarity (Select → Confirm → Success)  
Confirmation modal:  
“Are you sure you want to report this ID as lost/stolen/compromised?”  
Warning about penalties for false reporting  
Multilingual support for inclusivity (English, Hausa, Yoruba, Igbo)  
  
🎨 UI/Design  
Red accents for urgency & warnings  
Icons for each ID type (🪪 National ID, 🗳 Voter’s Card, 🚗 Driver’s License, 🌍 Passport)  
Clean wizard-style cards for each step  
Status indicator badges on ID preview:  
“Active” (green)  
“Lost” (yellow)  
“Stolen” (red)  
“Compromised” (orange)  
Success modal with reference number + next steps  
  
🛠 Technical Considerations  
API endpoint: POST /report-id  
Verification before final submission:  
PIN, OTP, or biometric (fingerprint/face scan)  
Database updates:  
is\_reported = true  
report\_reason = lost/stolen/compromised  
report\_date = timestamp  
Store uploaded documents securely (encrypted)  
Audit log: who reported, when, which ID, status change  
Integration with national lost/stolen ID database (shared with banks, telecoms, law enforcement)  
  
🚀 Scalability  
Support document recovery flow if ID is later found (reverse reporting)  
Add tracking reference number for citizen & agency follow-up  
Agent-facing interface for manual reports (offline offices, call centers)  
Bulk-reporting by agencies during disasters  
AI-based fraud detection: flag suspicious repeated reports  
Future: Integration with police/law enforcement database for real-time fraud prevention  
  
🔄 Suggested Flow  
Citizen Dashboard → Profile → ID Management → Report Lost/Stolen/Compromised → Fill Form → Confirm → Generate Reference Number → ID Deactivated → Notifications Sent → Option to Apply for Replacement  
  
✅ This way, it combines your detail-rich citizen safety features and my security/government process flow into one final, professional-grade documentation.  
✍ Digital Signature & Document Verification Page  
This page empowers citizens to digitally sign official documents and verify authenticity of government/partner documents using their secure NatioID digital identity.  
  
✅ Content  
Header: “Digital Signature & Document Verification”  
Two main tabs:  
Sign a Document  
Verify a Document  
Upload field (PDF, DOCX, JPG/PNG scans)  
Signature preview (citizen’s registered digital signature)  
Signing methods:  
Stored secure digital certificate/signature  
Biometric confirmation (fingerprint/face)  
Secure PIN entry  
Download signed file (with embedded signature/QR)  
Share options: Email, WhatsApp, Gov Portal  
QR code / hash string displayed for cross-verification  
  
⚙ Functionality  
Digitally attach unique citizen signature (PKI-based)  
Generate timestamp + unique signature ID  
Verify by uploading document or scanning QR/hash  
Validate via government backend (signature authenticity, timestamp integrity, issuer authority)  
Auto-log into Activity Timeline & Audit Trail  
  
🛡 Security  
Uses end-to-end encryption (AES + PKI)  
Signature bound to citizen’s NIN (non-transferable)  
Tamper-proof: any document change invalidates signature  
Secure cloud storage for signed docs (opt-in)  
  
🎨 UI/UX  
Clean dual-tab design (Sign vs Verify)  
Drag-and-drop OR file picker for uploads  
Live preview of digital signature before applying  
Confirmation modal with PIN/Biometric check before signing  
Clear success/failure verification states (✅ Verified / ❌ Invalid / ⚠️ Expired)  
  
🛠 Tech Considerations  
API endpoints:  
POST /sign-document  
POST /verify-document  
Support for PDF/A compliant signatures  
Hashing: SHA-256 or SHA-3 standard  
Blockchain (optional, future roadmap) for tamper-proof verification  
  
🚀 Scalability  
Multi-language document support  
Integration with government e-services (passport, tax, land registry, etc.)  
Future: interoperability with international e-sign frameworks (EU eIDAS, UNCITRAL)  
  
🔄 Flow  
Dashboard → Digital Services → Digital Signature → [Sign | Verify]  
  
🚑 Emergency Services Page  
This page provides instant access to national emergency services with an SOS function for critical help.  
  
✅ Content  
Emergency Numbers (tap-to-call):  
Police (112/NPF)  
Fire Service  
Ambulance/Medical  
NEMA (Disaster Response)  
Prominent SOS Button for immediate assistance  
Display/share user’s location (GPS)  
Emergency Profile: blood group, allergies, ICE contacts, medical conditions  
Silent Mode toggle (for discreet distress calls)  
  
⚙ Functionality  
One-tap call to listed emergency services  
SOS button triggers:  
Location auto-shared with authorities + ICE contacts  
SMS alert to predefined contacts with live location link  
Optional background audio recording for evidence  
Offline fallback: stores national emergency numbers locally  
Editable emergency medical profile  
Auto-log in Activity Timeline & Security Center  
  
🎨 UI/UX  
Red floating SOS button (persistent across app)  
High-contrast icons for readability in panic situations  
Simple one-page layout (no clutter)  
Confirmation screen with “Cancel in 3s” countdown to avoid false triggers  
  
🔐 Security  
Requests permission for location, contacts, microphone only when needed  
PIN/Biometrics required to cancel SOS (prevents forced cancellation)  
All alerts encrypted before transmission  
Logs all SOS activations for audit & analytics  
  
🛠 Tech Considerations  
API endpoints:  
POST /sos-alert  
POST /update-emergency-profile  
Geo-location API with fallback to GSM tower data  
SMS gateway integration for offline/low-data regions  
Push notification service for emergency responders  
  
🚀 Scalability  
Integration with state police & local emergency centers  
Future: add crowdsourced “nearby helpers” volunteer option  
Possible AI SOS detection (voice recognition: “help”, “fire”, “kidnap”)  
  
🔄 Flow  
Anywhere in app → Tap SOS → Confirm (3s) → Alert Sent → Help Dispatched  
📆 Activity Timeline Page  
Purpose  
A chronological log of all major user actions in the app, ensuring transparency, traceability, and security awareness.  
  
✅ Content & Actions  
Timestamps for each activity  
Activity type icons (🔐 Login, 🗳 Vote, 📷 Scan, ✍ Digital Signature, 🆘 SOS, ⚙ Profile changes)  
Filters:  
By date range  
By activity type (logins, votes, scans, changes, subsidies, etc.)  
Expandable entries: details include IP address, device, geolocation (if available)  
Visual format: vertical scrolling timeline with color-coded icons  
Export options: download as PDF/CSV for record keeping  
(Optional) Clear history button — configurable (some logs may remain system-only for integrity)  
  
🔐 Use Cases  
Users can review suspicious activity (failed logins, multiple location changes)  
Track own usage behavior over time  
Provides user empowerment over their digital identity  
Supports admin audit & fraud detection  
  
🎨 UX Notes  
Always accessible via Profile > Security > Activity Timeline  
Clear day dividers in timeline for readability  
Export option visible but deletion limited for integrity  
Real-time updates: new log entries appear instantly without reload  
  
🛠 Technical & Security  
API: GET /activity-log?userId with filters  
Logs stored encrypted & immutable (cannot be tampered by user)  
Alerts for anomalies (e.g., repeated failed login attempts)  
Pagination for large histories  
  
  
💰 Benefits & Subsidies Page  
Purpose  
A centralized hub for citizens to discover, apply, and track government-provided social benefits with real-time eligibility checks.  
  
✅ Content & Actions  
Benefit Categories:  
Pensions  
Healthcare schemes (NHIS, medical subsidies)  
Educational grants & scholarships  
Fuel/food subsidies & welfare transfers  
Agricultural support (loans, fertilizer subsidies)  
Each program card includes:  
Program name & description  
Eligibility status: Eligible, In Progress, Disbursed, Not Qualified  
Action buttons: Apply, Track, or Appeal  
Linked ID (NIN or supporting documents)  
Timeline of benefit applications: milestones like submitted → verified → approved → disbursed  
  
🛠 Features  
Eligibility check engine: evaluates user profile (age, occupation, income, disability, etc.)  
Integration with external government databases & welfare APIs  
Notifications for application updates and new subsidies  
Multilingual support for accessibility (English, Hausa, Yoruba, Igbo, etc.)  
Estimated disbursement dates shown for approved benefits  
  
🎨 UX Notes  
Group programs into categories with icons (💊 Healthcare, 🎓 Education, 👴 Pension, 🌾 Agriculture)  
Status shown with progress bar (Pending → Verified → Approved → Disbursed)  
New/closing soon programs highlighted with badges  
Applications shown in a history/timeline view  
  
🔐 Security  
Only verified NIN holders can apply  
All sensitive data encrypted in storage & transit  
Fraud prevention: one application per program per NIN  
Data access restricted to authorized government bodies  
  
🛠 Technical Considerations  
API Endpoints:  
GET /benefits → list of programs  
POST /apply-benefit → submit application  
GET /benefit-status/:id → check status  
Real-time status updates via push notifications  
Integration with payment/wallet systems for disbursements  
📢 News & Updates / Government Feed Page  
Purpose  
Keep citizens informed with verified government-backed information about policies, reforms, subsidies, and ID-related updates.  
Content  
Policy announcements & reforms  
National ID program updates  
Subsidy & social welfare news  
Multimedia: images, videos, infographics  
Date-stamped & verified articles  
Functionality  
Category filters: ID, Health, Education, Election, Subsidies  
Search & bookmark articles  
Push alerts for breaking news  
Social media sharing  
Offline caching (optional)  
Accessibility options: text resize, narration, multi-language support  
UI/UX  
Scrollable card-based feed  
“Read More” expandable summaries  
Highlight urgent alerts in red/bold  
Mobile-first design with clean typography  
Tech Considerations  
CMS/Admin Dashboard for government officials to push updates  
Content verification + metadata logging  
Scalable API for media (text, images, video)  
  
📊 Economic Dashboard Page  
Purpose  
Provide transparent, real-time national economic indicators for citizens to stay informed.  
Content  
Inflation, unemployment, fuel & FX rates  
Subsidy allocations & disbursement stats  
Economic forecasts & trends  
Regional breakdown (state/zone-level)  
Functionality  
Interactive graphs & charts  
Filter by time range (daily, monthly, yearly)  
Export reports (PDF/CSV)  
Personalized regional views (optional)  
Tooltips for quick breakdowns  
UI/UX  
Visual dashboards with graphs, maps, infographics  
Color-coded indicators: Green = Healthy, Red = Warning  
Mobile-friendly, responsive layouts  
Tech Considerations  
API integration with economic/statistical bodies (CBN, NBS)  
Auto-refresh with live/scheduled updates  
Scalable for future economic data (housing, trade, GDP)  
  
🔔 Notification Center Page  
Purpose  
Centralize all notifications sent to the citizen from within NatioID.  
Content  
Categorized alerts:  
Security: SOS, fraud, breach attempts  
Government: reforms, policies, news  
Financial: subsidy eligibility, payments  
Personal: account activity, ID expiry reminders  
Functionality  
Filter by category/date  
Mark as read/unread  
Push notification toggle  
Search notifications  
Swipe to archive/delete  
UI/UX  
List view with unread badges  
Category tabs (All, Security, Govt, Financial, Personal)  
Clear timestamping  
Accessible, mobile-first layout  
Tech Considerations  
Notification queue + delivery system (e.g., Firebase, OneSignal)  
Encryption for sensitive alerts  
Option to sync across devices  
  
🗂 Application Tracking Page  
Purpose  
Allow citizens to track the real-time progress of government service applications (passport, subsidies, licenses, benefits, etc.).  
Content  
Application type (e.g., Passport, Voter Card, Subsidy)  
Reference number / Tracking ID  
Submission date  
Status: Received, In Review, Approved, Rejected, Completed  
Progress timeline (step tracker)  
Expected completion date  
Contact officer info (optional)  
Uploaded documents (view/download)  
Status history log  
Functionality  
Filter by application type/status  
Upload additional docs (if requested)  
Push notifications on progress updates  
Download application summary (PDF)  
Re-submit if rejected (optional)  
QR code for quick office scanning  
Track via tracking ID (without login)  
UI/UX  
Stepper-style status tracker + progress bar  
Color-coded states: Gray = Pending, Blue = In Progress, Green = Approved, Red = Rejected  
Mobile-first design  
Icons for each application type  
Security  
Encrypted data & documents  
Access limited to applicant + authorized staff  
Audit trail of all changes  
Scalability  
Expandable to new application types (permits, housing, business licenses)  
Government admin dashboard for updates  
API integration with back-office systems  
  
  
🇳🇬 NatioID – Project Specification  
A civic portal web app for Nigeria that provides secure digital identity, citizen services, benefits tracking, and real-time government communication.  
  
✅ MVP Features (Phase 1 – Launch Ready)  
1. Core Identity & Security  
NIN-based login + OTP authentication.  
Biometric login (Face ID, fingerprint).  
Active Sessions list (manage & log out remotely).  
Encrypted local storage (no sensitive caching).  
2. Emergency & Safety Hub  
Unified page: SOS button, Emergency Services directory, Security Alerts.  
Trusted Contacts → auto-notify selected family/friends during SOS.  
Geo-location sharing with consent.  
3. Citizen Profile & ID  
Digital ID card (print/download PDF).  
QR Code verification (for scanning by officials).  
Profile image + basic citizen details.  
4. Activity & Audit Timeline  
Chronological log of actions (logins, votes, scans).  
Filter by type (e.g., “Votes only”, “Logins only”).  
Export to CSV/PDF (Phase 2 upgrade).  
5. Benefits & Subsidies  
Grants, pensions, healthcare, education benefits.  
Status tracking: Eligible, Pending, Disbursed, Not Qualified.  
Document upload for eligibility.  
Appeal/Resubmit workflow.  
6. Application Tracking  
Track government services (passport, subsidies, benefits).  
Status indicators (color-coded: green/yellow/red).  
Estimated processing times.  
7. News & Government Updates  
Feed of national policies, reforms, subsidies.  
Multi-language support (English, Hausa, Yoruba, Igbo).  
Text-to-speech accessibility.  
8. Notification Center  
Inbox-style: read/unread + archive/clear all.  
Filters: All, Security, Govt, Financial, Personal.  
9. Digital Consent & Legal  
Consent prompts for sensitive actions.  
Centralized Terms & Conditions page.  
  
🔁 Phase 2 Features (Expansion)  
Identity & Security  
PKI-backed Digital Signature for documents.  
Government seals/stamp validation.  
Emergency Hub  
Geo-fencing alerts (optional + opt-in).  
Push notifications with urgency levels (Critical, Important, Informational).  
Economic Dashboard  
Market data, inflation rates, subsidy allocations.  
“Pro View” with analytics for researchers/analysts.  
Activity & Timeline  
Full export options (PDF/CSV).  
Advanced filters (by date range, activity type, location).  
Applications & Benefits  
Deeper integration with gov APIs for auto-status updates.  
Integration with mobile money/bank APIs for disbursement alerts.  
  
🎯 Cross-Cutting UX Enhancements  
Consistent green-white Nigerian theme (coat of arms watermark, modern UI).  
Accessibility-first: narration/screen-reader tags, high contrast mode, large text support.  
Multi-language translation across all modules.  
Trusted Contacts & family linkage features for emergencies.  
  
📌 Development Roadmap  
Sprint 1 – Core Infrastructure  
Authentication (NIN, OTP, Biometric).  
Profile & Digital ID (QR + Print).  
Core Database (Citizen, Applications, Benefits, Logs).  
Sprint 2 – Citizen Services  
Emergency & Safety Hub.  
Benefits & Subsidies (basic tracking).  
Application Tracking.  
Sprint 3 – Engagement & Transparency  
Activity Timeline.  
News & Government Updates.  
Notification Center.  
Sprint 4 – Security & Expansion  
Consent & T&Cs integration.  
Advanced security: Active Sessions, session termination.  
MVP polishing + accessibility/language rollout.  
Phase 2 – Post-Launch  
Digital Signature (PKI).  
Economic Dashboard (Pro Mode).  
Geo-fencing + push notifications.  
Timeline export & advanced analytics.  
  
  
🧑‍💼 Admin / Government Portal  
Core Modules  
Dashboard (Overview)  
KPIs: Citizens onboarded, active IDs, pending verifications.  
Alerts: SOS requests, fraud flags.  
Graphs: Registrations over time, voting stats, subsidy uptake.  
Quick actions (Verify ID, Publish Announcement).  
Citizen Management  
Search/filter citizen profiles.  
View/Edit details (role-based).  
Link multiple IDs (NIN, Voter Card, Passport).  
Status: Active / Flagged / Suspended.  
Export records.  
ID Verification Center  
Review pending ID submissions.  
Approve / Reject / Request reupload.  
Audit trail of actions.  
Application Management  
Track all applications (passport, subsidies, pensions).  
Status: Pending, Approved, Rejected.  
Bulk actions + SLA tracking.  
Internal comments/notes.  
Election Oversight (optional/phase 2)  
Candidate profile management.  
Live monitoring of turnout.  
Region-wise voting heatmap.  
Emergency Alerts & SOS  
Live map feed of SOS signals.  
Assign to agency.  
Mark resolved + escalate if needed.  
Trusted contacts alert history.  
News & Public Updates  
Publish announcements to citizens.  
Categorize (Policy, Health, Elections, Economy).  
Schedule + attach media.  
Benefits & Subsidy Center  
View applications with uploaded docs.  
Approve/Reject/Request proof.  
Handle appeals.  
Analytics by region & category.  
Complaints & Feedback  
Ticket-style system (assign, resolve).  
Categorize by sector/agency.  
SLA timers + escalation matrix.  
Analytics on complaints per region.  
Document & Signature Verification  
Verify uploaded signed docs.  
Cross-check QR/Barcode authenticity.  
Issue official digital seals.  
Audit Logs / Activity Timeline  
All admin actions logged.  
Role, IP, timestamp.  
Export for compliance/legal review.  
Admin User Management  
Create/edit/remove admins.  
Role-based permissions (SuperAdmin, State Official, Local Gov).  
Track admin activity.  
Notification Center  
Create citizen notifications.  
Target filters: nationwide, state, specific groups.  
Schedule or instant push.  
Settings  
Global system configs (data retention, ID types).  
Maintenance mode toggle.  
Branding, theme, logos.  
🔑 Final Review (Admin Portal)  
RBAC Matrix → Well-structured.  
✅ Suggestion: Add a “Read-only Auditor” role (e.g., for independent monitors / anti-corruption agencies). They can view but not edit. This prevents tampering while boosting trust.  
Escalation Matrix → Excellent accountability.  
✅ Suggestion: Add SLA dashboard for admins → color-coded timers (green/orange/red) to show if issues are about to breach SLA.  
Analytics Layer → Strong.  
✅ Suggestion: Add “Custom Query Builder” so superadmins can generate ad-hoc reports without needing dev support.  
Export & API Access → Critical.  
✅ Suggestion: Add expiry dates + revocation controls for API tokens. Helps manage inter-agency integrations securely.  
Cross-linked Records → Great for 360° citizen view.  
✅ Suggestion: Add “Case Notes” field so admins can leave private notes tied to citizen cases (visible only to authorized staff).  
Dark Mode & Accessibility → Strong UX.  
✅ Suggestion: Add offline fallback mode (limited view of last synced data) for rural areas where admins may lack connectivity.  
Multi-language & Localisation → Inclusive.  
✅ Suggestion: For admin portal, allow translation keys but default English-only, so future scaling to other regions (e.g., ECOWAS) is easy.  
  
🛠 Additional Admin-Side Enhancements  
Audit Log by Role & Action  
Every login, data export, edit, or escalation should be recorded. This protects against insider threats.  
Admin-to-Admin Messaging/Notes  
A lightweight secure chat for escalation handovers (instead of relying on external tools like WhatsApp).  
Citizen Privacy Guard  
Certain sensitive data (e.g., health, financial aid) should require dual approval before editing (two admins verify).  
Layout Differentiation  
Citizen Layout → clean, mobile-first, green-white themed, card/timeline-based.  
Admin Layout → dashboard-style, sidebar navigation, data tables, analytics panels.  
✅ Suggestion: Ensure both follow consistent design language, but with different emphasis: simplicity for citizens, power tools for admins.  
  
✅ Final Summary Table  
  
👉 With these refinements, your citizen + admin ecosystem is now:  
Secure 🔐  
Scalable 📈  
Inclusive 🌍  
Usable in real-world Nigerian contexts 🇳🇬  
  
  
🏛 Admin Portal – Pages, Features & Functionality  
  
1. Dashboard (Overview)  
Contents  
KPIs: total citizens, active IDs, pending verifications, subsidy count.  
Graphs (registrations trend, voting stats, complaints trend).  
Alerts: pending SOS, flagged IDs, unresolved complaints.  
Features & Functionality  
Click KPIs → drill down to detail pages.  
Quick Actions: Approve ID, Publish Announcement, View SOS.  
Toggle dark/light mode.  
Accessibility controls (font size, screen-reader).  
  
2. Citizen Management  
Contents  
Search bar (NIN, Name, Phone, Region).  
List of citizens with status (Active / Pending / Suspended).  
Tabs: Profile | Applications | Benefits | Complaints | Audit.  
Features & Functionality  
View full citizen profile.  
Edit non-core fields (based on admin role).  
Suspend / reinstate account.  
Export list (CSV/PDF).  
RBAC ensures only authorized edits.  
  
3. ID Verification Center  
Contents  
Queue of pending ID submissions.  
Details: photo, document scans, NIN.  
Fraud/flag indicators.  
Features & Functionality  
Approve, Reject, Request Reupload.  
Auto-validation checks (duplicate NIN, expired docs).  
Audit log for every action.  
Escalate suspicious IDs.  
  
4. Application Management  
Contents  
All applications (passports, subsidies, pensions, scholarships).  
Filters: type, region, status.  
Status: Pending | Approved | Rejected.  
Features & Functionality  
Bulk actions (approve/reject).  
SLA timer display (time left to respond).  
Add internal notes for colleagues.  
Auto-escalate if idle > set time.  
  
5. Election Oversight (Phase 2)  
Contents  
Candidate profiles.  
Real-time voting dashboard.  
Region-wise turnout map.  
Features & Functionality  
Add/verify candidates.  
View voting stats by state/LGA.  
Fraud detection alerts (duplicate votes).  
Export election data.  
  
6. Emergency Alerts & SOS  
Contents  
Live map of SOS alerts.  
Citizen details + location.  
Status: Active, Assigned, Resolved.  
Features & Functionality  
Assign SOS to agency.  
Mark resolved or escalate.  
Trusted contacts auto-alert log.  
Escalation Matrix (Local → State → National).  
  
7. News & Public Updates  
Contents  
Announcement editor (title, content, media).  
Categories (Policy, Health, Elections, Economy).  
Publish history.  
Features & Functionality  
Publish instantly or schedule.  
Multi-language toggle (EN, HA, YO, IG).  
Attach images/videos.  
Archive past updates.  
  
8. Benefits & Subsidy Center  
Contents  
Citizen subsidy applications.  
Uploaded documents.  
Appeal/resubmit records.  
Features & Functionality  
Approve/Reject/Request more docs.  
Mark fraud or duplicate cases.  
Generate reports by category/region.  
Visualize subsidy distribution (heatmap).  
  
9. Complaints & Feedback  
Contents  
Complaint tickets list.  
Citizen info, complaint details.  
SLA timer.  
Features & Functionality  
Assign to department.  
Add resolution notes.  
Escalate overdue complaints.  
Export complaints dataset.  
  
10. Document & Signature Verification  
Contents  
Uploaded citizen docs.  
QR/Barcode scan field.  
Verification results.  
Features & Functionality  
Validate authenticity.  
Issue official digital seals.  
PKI integration for digital signatures.  
Log all verification attempts.  
  
11. Audit Logs / Activity Timeline  
Contents  
All admin actions logged.  
Filters by date, user, action type.  
Features & Functionality  
Export logs (PDF/CSV).  
Merge view with Activity Timeline.  
Role/IP/time tracking.  
Highlight suspicious activity.  
  
12. Admin User Management  
Contents  
List of all admin accounts.  
Roles: SuperAdmin, National Officer, State Officer, Clerk.  
Status (Active, Suspended).  
Features & Functionality  
Add/Edit/Delete admins.  
Assign permissions by role.  
View admin activity logs.  
Active Sessions list (force logout).  
  
13. Notification Center  
Contents  
Citizen notification drafts.  
Scheduled & sent notifications.  
Target filters (region, age, gender, occupation).  
Features & Functionality  
Create new notification.  
Push instantly or schedule.  
Inbox-style archive + clear all.  
Track delivery success/fail rate.  
  
14. Settings  
Contents  
System-wide settings.  
Branding (logo, theme).  
Data retention policies.  
Features & Functionality  
Enable/disable modules (e.g., Election).  
Maintenance mode.  
Configure i18n (multi-language).  
Manage dark/light themes.  
  
15. Data & Analytics Hub  
Contents  
Subsidy distribution heatmap.  
Complaint category charts.  
Voting trends.  
Fraud detection dashboard.  
Features & Functionality  
Filter by time/region.  
Export insights (CSV/PDF).  
Compare historical vs real-time data.  
Share dashboards with government agencies.  
  
16. API & Data Exchange  
Contents  
API keys list.  
Access logs.  
Dataset exports.  
Features & Functionality  
Generate scoped API tokens.  
Limit usage per agency/partner.  
Export datasets securely.  
View API request history.  
  
👉 That’s a page-by-page functional breakdown for the entire Admin Portal.  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
  
📌 Updated Changes Needed  
1. Restructure Into Phases (Scope Control)  
Add a new page/section called “Release Phases / MVP Roadmap” after the intro.  
Content:  
Phase 1 (MVP – ~20 pages)  
Onboarding, Login, Digital ID Wallet, Linked Services (basic), Complaint Tracking, Security Alerts/SOS, Basic Dashboard.  
Phase 2  
Voting (secure casting + history), Benefits & Subsidies, Verification Center, Extended Linked Services.  
Phase 3  
Advanced features: Blockchain audit logs, AI fraud detection, NFC ID scan, Biometric Match, Admin Analytics.  
  
2. Security & Compliance Enhancements  
Add a new page “Data Security & Compliance Framework”.  
Content:  
Data retention (how long citizen logs/complaints are stored).  
Consent revocation policy.  
NDPR/GDPR alignment.  
Government/legal escalation workflow.  
Audit log immutability (specify which logs can never be deleted).  
  
3. Technical Architecture View  
Add a page “System Architecture Overview” before the individual page specs.  
Content:  
Diagram:  
Mobile App ↔ API Gateway ↔ Services (Auth, Citizen Profile, Voting, Complaints, Notifications) ↔ DB.  
Call out integrations: NIMC (NIN), INEC (Voting), NHIS, Banks.  
Offline flow (local cache → sync).  
  
4. Data Models / Entities  
Add a new “Core Data Models” page.  
Include tables for:  
Citizen (id, nin, name, dob, phone, email, status).  
Complaint (id, citizen\_id, type, description, status, response, created\_at).  
VerificationLog (id, citizen\_id, entity, purpose, status, timestamp).  
ElectionVote (id, election\_id, citizen\_id, candidate\_id, encrypted\_vote, timestamp).  
LinkedService (id, citizen\_id, service\_name, data\_shared, status).  
  
5. API Contracts / Examples  
For each functional module (Auth, ID, Complaints, Voting), add sample endpoints + request/response.  
E.g.,  
POST /api/complaints/submit  
{  
 "citizen\_id": "12345",  
 "type": "Lost ID",  
 "description": "My card is missing",  
 "attachment\_url": "https://..."  
}  
Response:  
{  
 "complaint\_id": "CMP-2025-0001",  
 "status": "pending"  
}  
  
6. Admin Portal (New Section)  
Add a dedicated section: “Admin Dashboard & Workflows”.  
Pages:  
Admin Login.  
Citizen Data Correction Requests.  
Complaint Resolution Workflow.  
Verification Monitoring Dashboard.  
Security Alerts & Fraud Detection.  
  
7. Voting Page Adjustments  
Current doc suggests live vote casting + blockchain audit.  
Revise to:  
MVP: Voting page = Eligibility check + Candidate info + Live results (read-only).  
Phase 2: Enable secure encrypted vote casting with PIN+biometric.  
Phase 3: Blockchain-backed audit + turnout analytics.  
  
8. Trim Heavy Features for Later  
Move these to Phase 3 appendix (not MVP):  
NFC ID Scan.  
Blockchain-backed logs.  
AI fraud detection.  
Advanced biometrics (multi-device, face match).  
International integrations (ICAO, cross-border ID).

## Updated Version (Merged with Additions)

Citizen App (35 Pages):  
- Registration → OTP → PIN → Biometric → Dashboard  
- Digital ID Wallet (QR, blur privacy, share/download)  
- Linked Documents (passport, driver’s license, voter card, insurance)  
- ID Applications (new, renewal, lost/stolen tracking)  
- Voting (Election type → Candidate → Cast vote → Success/Error → Live Results)  
- News & Benefits (categories, save, filter)  
- Complaints/Reports (submit, track, resolve)  
- Notifications (push, reminders, renewal alerts)  
- Settings (theme, language, account recovery, privacy)  
- Extra Features: Theme & Language switcher, Screenshot prevent, Clipboard restrict, App blur, Offline mode  
  
Admin App (16 Pages):  
- Login → Dashboard  
- Citizen Applications (review, approve, reject)  
- Documents (verify, reject)  
- Complaints (view, resolve)  
- Voting Management (create election, add candidates, monitor live)  
- News & Benefits (publish, categorize)  
- Notifications (push to users)  
- Activity Logs (audit actions)  
- Reports (usage, fraud, compliance)  
- RoleAdaptation: Admin (approve/manage), Reviewer (view/comment), Viewer (read-only)  
  
Super Admin Module:  
- Pages: Login, Dashboard, Admin Accounts Management, Admin Detail, Admin Activity Logs, System Settings, Audit Reports  
- Functions: Manage admins (add, edit, suspend, delete), Assign/revoke roles, Configure system (branding, registration rules), Generate compliance reports, Oversight of logs  
  
RBAC System:  
- Roles: SuperAdmin, Admin, Reviewer, Viewer  
- Permissions: applications:create/read/update/status, documents:verify/reject, users:read/manage, news:publish, voting:create/manage/live, system:settings, audit:read/export  
- UI Behavior: Frontend hides/disables buttons per role, backend enforces permissions  
  
APIs:  
- Auth: register, verify-otp, login, refresh, 2FA  
- Users: profile, update, status  
- Applications: apply, renew, status, admin review  
- Documents: upload, verify, status  
- Voting: list elections, candidates, cast vote, results  
- News: list, publish, categorize  
- Complaints: submit, resolve  
- Notifications: push, list  
- SuperAdmin: manage admins, roles, settings, reports  
  
Security:  
- JWT + refresh, Rate limiting & IP logging, Idempotency keys (voting & apps)  
- Immutable audit logs, Biometric + OTP before sensitive actions  
  
DevOps:  
- OpenAPI 3.0 docs (Swagger UI), Dummy endpoints preserved  
- Staging before production, CI/CD pipelines, Rollback plan, Monitoring + backups