NEST — ENGINEERING DESIGN DOCUMENT

Authentication, Authorization & Accounting (AAA)

Version 1.0 — November 2025

This document defines the authentication and authorization framework for the Nest Digital Cooperative Ecosystem. It ensures multi-channel access (USSD, WhatsApp, Web) with unified identity and MFA-enabled security.

1. Overview

Nest Version 1 introduces a unified authentication and authorization framework across USSD, WhatsApp, and Web channels. Each user has a unique identity (`user_id`), ensuring consistent access, auditability, and secure transactions across platforms.

Table: MFA Enforcement per Channel

Channel	Primary Factor	Secondary (MFA)	When Applied
USSD	MSISDN + PIN	OTP (SMS)	Loan requests, disbursements
WhatsApp	Linked Number	OTP (SMS/WA)	High-value approvals
Web	Password	OTP (new device)	Always on first device
Bank Official	Password	TOTP	Always required
Nest Staff	SSO	TOTP	Always required

2. API Endpoint Examples

POST /auth/request-otp — Request OTP for registration, login, or approval.

```
Request: { "phone": "+254712345678", "context": "registration" } Response: { "status": "OTP_SENT", "expires_in": 300 }
```

POST /auth/verify-otp — Validate OTP for verification.

```
Request: { "phone": "+254712345678", "otp": "123456" } Response: { "status": "VERIFIED", "user_id": "USR-100234" }
```

3. Security Implementation Notes

• All passwords and PINs are hashed using Argon2id or bcrypt. • Data in transit is secured with HTTPS (TLS 1.3). • All sensitive data (bank account numbers, IDs) is AES-256 encrypted at rest. • OTPs are valid for 5 minutes and cached in Redis. • Every authentication and approval event is logged with IP, timestamp, and channel.

4. Audit Logging Example

```
{ "event": "OTP_VERIFICATION", "user_id": "USR-CHAIR-234", "channel": "web",
"timestamp": "2025-11-11T19:22:54Z", "result": "success" }
```

5. Future Enhancements (Version 2+)

• Behavioral Risk Scoring — AI-driven anomaly detection on unusual logins (geo/device). • Device Fingerprinting — Browser/device tracking for suspicious access. • Biometric MFA — Fingerprint or FaceID for Mobile (Version 3). • Delegated Access — Temporary delegation of Chama roles.