Veriqo – Full Design & Architecture Conversation

This document contains the complete consolidated content of the design conversation covering system architecture, workflows, reporting, PDF generation, QR access, branding, and final naming for the Veriqo platform.

1. Purpose & Vision

Veriqo is a white-label console verification and refurb platform designed for professional repair, refurbishment, and resale operations. It focuses on traceability, evidence, and process enforcement rather than OEM-level diagnostics.

2. Core Architecture

Frontend: React (Vite, TypeScript), tablet-first.

Backend: FastAPI with JWT authentication.

Database: PostgreSQL with Alembic migrations.

Evidence Storage: Local filesystem.

Reporting: ReportLab-generated PDFs with QR access.

3. Workflow

Station-based workflow: Intake → Reset → Functional → QC.

Each device equals one Job. Jobs move sequentially with gated steps, mandatory evidence, and technician accountability.

4. Data Model Overview

Key entities: users, devices, jobs, stations, test_steps, test_results, evidence, reports.

Reports support customer/internal variants, per-station and master scope, token-based public access, and expiration handling.

5. Evidence & Compliance

Evidence (photos/videos) is mandatory for critical steps such as factory reset.

Evidence is hashed, timestamped, and linked to jobs and steps for auditability.

6. Reporting System

Veriqo generates white-label PDF reports per job.

Each job can produce customer and internal reports across all scopes (master, intake, reset, functional, QC).

Reports include device data, summary metrics, test tables, reset image thumbnails, QC initials, and a QR code for public access.

7. QR & Public Access

Each report is assigned a cryptographically secure token.

Public access via /r/{token} without authentication.

Default expiration: 90 days.

8. Branding

Final selected brand name: Veriqo.

White-label design with optional logo. If no logo is present, a placeholder is rendered.

Theme color and brand name are environment-configurable.

9. Security Model

JWT-based role access control.

Public report access is token-based with expiry.

Internal endpoints require authenticated roles.

10. Current State

The system design and implementation plan are complete.

All major components are specified and ready for deployment, iteration, and extension (Switch, Xbox, analytics, auto-reporting).

Appendix: Naming Decision

After evaluating trademark risk and branding strategy, the platform name 'Veriqo' was selected. Veriqo is a coined term with very low trademark collision risk, suitable for international B2B use and white-label certification reporting.