Finanzas Auth + API E2E Validation (Hosted UI → Callback → AuthProvider → API)

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 14, 2025

1 Finanzas Auth + API E2E Validation (Hosted UI → Callback → AuthProvider → API)

Last updated: 2025-11-23T18:43:38Z

This run focuses on the end-to-end Finanzas authentication and API wiring with the existing Cognito implicit-flow design. The checks are organized by the layered plan (Hosted UI/Callback, AuthProvider bridge, HTTP client/API). AWS-side validation remains required; see the **Pending AWS validation** notes where console-side testing could not be executed from this environment.

1.1 Layer 1 – Hosted UI → Callback

Files inspected - `src/config/aws.ts` (Hosted UI params) - `public/finanzas/auth/callback.htm` (canonical static callback handler) - `public/auth/callback.html` (legacy entry point) - `src/App.tsx` (callback guard)

Findings and changes - Added hardened defaults in `src/config/aws.ts` so the documented Cognito settings remain in place even if environment variables are absent: region `us-east-2`, user pool `us-east-2_FyHLtOhiY`, client ID `dshos5iou44tuach7ta3ici5m`, domain `us-east-2fyhltohiy.auth.us-east-2.amazonaws.com`, and CloudFront base `https://d7t9x3j66yd8k.cloudfront.net`. The Hosted UI URL construction now resolves to the expected implicit-flow authorize URL out of the box. - Restored the canonical callback path under `public/finanzas/auth/callback.html` (the file the Hosted UI is configured to hit). The existing logic remains unchanged: it parses `id_token`/`access_token` from the hash, stores `cv.jwt`/`finz_jwt`/`idToken`/`cognitoIdToken`, and redirects to `/finanzas/`. - Converted the legacy `public/auth/callback.html` into a thin redirector that preserves both query and hash fragments and forwards to `/finanzas/auth/callback.html`. This prevents Cognito tokens from being lost if someone bookmarks the legacy path while keeping a single source of truth for callback processing. - Router guard in `src/App.tsx` already short-circuits any `/auth/callback` route so React will not intercept the static callback; no change needed.

AWS validation (pending) - Hosted UI login via the Cognito console ("Try hosted UI") → `https://d7t9x3j66yd8k.cloudfront.net/finanzas/auth/callback.html#id_token=...` — *Not runnable from this container; must be exercised in AWS with a test user.*

1.2 Layer 2 – AuthProvider / useAuth bridge

Files inspected - `src/components/AuthProvider.tsx` - `src/hooks/useAuth.ts` - `src/hooks/useRole.ts` - `src/components/LoginPage.tsx`

Findings - AuthProvider bootstraps from the same keys the callback writes (`cv.jwt` → `finz_jwt` → `idToken` → `cognitoIdToken`) and sets `isAuthenticated` after validating the JWT. Loading guards already prevent redirect loops while initialization runs. -

Hosted UI button on the login page calls `loginWithHostedUI()` directly; no localhost or react-oidc-context remnants detected.

AWS validation (pending) - After completing the Hosted UI login above, confirm `/finanzas/` renders authenticated state and localStorage contains the token keys. *Requires browser check against CloudFront.*

1.3 Layer 3 – HTTP client & Finanzas API wiring

Files inspected - `src/lib/http-client.ts` - `src/api/client.ts` - `src/api/finanzas.ts` - `infra/cloudfront-function-finanzas-rewrite.js` (callback bypass)

Findings - Central HTTP helpers already pull the bearer token from `cv.jwt/finz_jwt` (with fallbacks) and attach `Authorization: Bearer <jwt>` to Finanzas API calls using `VITE_API_BASE_URL`. - No code changes were required in this layer for token propagation; the canonical callback path alignment ensures the expected keys are populated before requests run.

AWS validation (pending) - API Gateway test (e.g., `GET https://pyorjw6lbe.execute-api.u` with `Authorization: Bearer <id_token>`). *Must be run via AWS console/CloudShell with a live Cognito token.* - Browser-side Network tab checks on Projects/Catalog/Invoice/SDMT after login to confirm 200 responses with the bearer token attached. *Requires CloudFront session.*

1.4 Commands to run

- `npm run lint`
- `npm run build:finanzas`

Run the above locally to confirm the build and lint gates remain green.

1.5 Evidence to capture when running AWS-side

- Hosted UI console login showing redirect to `/finanzas/auth/callback.html#id_token=...` and console logs `[Callback] id_token present: true`.
- API Gateway/CloudShell invocation returning 200 with the bearer token from Cognito.
- Browser Network tab showing authenticated Finanzas pages (Projects, Catalog, Invoice, SDMT) loading with `Authorization: Bearer …` headers.

1.6 Summary

- Root cause surfaced in this pass: the canonical `/finanzas/auth/callback.html` asset was missing, causing the configured Cognito redirect to hit a non-existent path. Added the canonical file back, ensured legacy paths forward to it, and

locked in the Cognito defaults so Hosted UI URLs resolve correctly even when environment variables are incomplete. Remaining verification must occur in AWS to confirm the end-to-end journey with real tokens and API responses.