

# **Finanzas Auth Flow Notes**

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 5, 2025

## 1 Finanzas Auth Flow Notes

### 1.1 Canonical token storage

- **Preferred access token:** `finz_access_token` (Cognito access token written by the hosted UI callback or `USER_PASSWORD_AUTH` login).
- **ID token fallbacks:** `cv.jwt`, `finz_jwt`, `idToken`, `cognitoIdToken` (used when no access token is available).
- The API client and AuthProvider read these keys from `localStorage` (and `sessionStorage`) in the order above.
- Build-time tokens (e.g., `VITE_API_JWT_TOKEN`) are only used for CI/E2E.

### 1.2 Error categories surfaced to the UI

- **AuthError (401/403):** Missing/expired token or forbidden action. The UI redirects to login and shows “Tu sesión ha expirado” or “No tienes permiso”.
- **ValidationError (400/422):** Input/contract issues. The UI shows the server-provided validation message.
- **ServerError ( $\geq 500$ ):** Unexpected backend failures. The UI shows a generic “Error interno de Finanzas” while logging details to the console (no secrets).

### 1.3 Diagnostics

- In development, each API call logs method, path, status, and a small response summary.
- Auth failures log a safe hint: “[Finanzas] Auth error from API (401). Likely missing/expired token – redirecting to login.”