Finanzas Authentication Notes

Finanzas SD – Architecture, Flows & SOPs

Arquitectura, Flujos y Procedimientos

December 6, 2025

1 Finanzas Authentication Notes

1.1 Token Storage

- **cv.jwt**: Primary JWT used by AuthProvider for session bootstrap.
- **finz_jwt**: Finanzas legacy key kept in sync with `cv.jwt` for compatibility.
- **idToken / cognitoIdToken**: Historical fallbacks still read by AuthProvider to avoid orphaned sessions.
- **finz_refresh_token**: Refresh token saved after USER_PASSWORD_AUTH logins when Cognito returns it.
- **finz_access_token**: Optional access token captured from the Hosted UI implicit flow for debugging/API tooling.
- **Sign-out behavior**: `signOut()` clears every token key above (including legacy fallbacks) plus the module preference (`cv.module`) to prevent stale sessions from silently re-authenticating after logout.

1.2 AuthProvider Decisions

- Auth is considered **authenticated** when a valid, non-expired JWT is found in any of the token keys above.
- Available roles are derived from Cognito groups → mapped to `PMO`, `SDMT`, `VENDOR`, `EXEC_RO`.
- `currentRole` persists in `user-current-role`; `cv.module` tracks PMO vs Finanzas preference for dual-role users.

1.3 useRole Behavior

- `useRole()` is a thin wrapper over `useAuth()` and simply surfaces `currentRole`, `setRole`, `availableRoles`, and a convenience `hasRole` check.
- Route guards should rely on `useAuth()`/`useRole()` and wait for `isLoading === false` before redirecting.

1.4 Hosted UI Flow (Implicit Grant)

- `loginWithHostedUI()` builds `https://<domain>/oauth2/authorize` with:
  - `response_type=token` (implicit grant)
  - `scope=openid email profile` (openid is required for `id_token`)
  - `redirect_uri=<CLOUDFRONT>/finanzas/auth/callback.html`
- Cognito returns `#id_token=...&access_token=...` in the hash fragment.
- `public/finanzas/auth/callback.html` parses the hash, requires `id_token`, stores tokens using the keys above, and redirects based on Cognito groups and `cv.module`

preference.

1.5 Custom Login Flow

- Username/password login uses `loginWithCognito()` (USER_PASSWORD_AUTH) and stores the same token keys as the Hosted UI flow.
- After login, AuthProvider decodes the JWT, sets roles, and redirects using the same group logic as the callback handler.