

Azure DevOps PAT — rotacija, auth putevi i anti-leak pravila

Azure DevOps PAT — rotacija, auth putevi i anti-leak pravila

Zadnja rotacija: 2026-07-17 (MC #103838) · **Org:** dev.azure.com/alai-holding · **SSOT za PAT:** Bitwarden item "Azure DevOps PAT - alai-holding" (776a5d5e)

Kanali koji RADE

1. **PAT preko REST-a:** `curl -u ":$PAT" https://dev.azure.com/alai-holding/_apis/projects?api-version=7.1` → 200.
2. **PAT preko git-a (header-auth, NIKAD u URL/config):**

```
B64=$(printf ':%s' "$PAT" | base64)
GIT_TERMINAL_PROMPT=0 git -c credential.helper= \
  -c http.extraHeader="Authorization: Basic $B64" \
  push https://x@dev.azure.com/alai-holding/Bilko/_git/Bilko <branch>:<branch>
```

Bez `credential.helper=` disable i dummy usera (`x@`) git ide u keychain/prompt uprkos `extraHeaderu`.

Kanali koji NE RADE (testirano 2026-07-17, ne pokušavaj ponovo)

- **SP alai-cli-deployer** (default az profil): ARM token validan, ali SP **nije član azdo org-a** → git vraća zavaravajuće "PAT expired". Fix = org admin doda SP u org.
- **AAD user Bearer (alem@alai.no):** azdo 403 "Identity has not been materialized" dok se taj identitet prvi put ne prijavi u org kroz browser. Org pristup u browseru ide preko drugog (radnog) naloga.

- **azdo SSH:** nijedan ključ registrovan.
- **FORGE "system az login":** STALE referenca — FORGE nema az profil; ado-agent-bilko koristi vlastiti OAuth RSA.

Rotacija (runbook)

1. Simptom: git push / azdo-merge-pr.sh / PR REST → 401. **Prvo provjeri PAT expiry REST-om** (`curl -u ":$PAT" .../_apis/projects` → "has expired").
2. CEO kreira novi PAT u browser UI (User settings → Personal access tokens; scope Code R/W + Build, 90 dana).
3. Verifikuj ŽIVO: projects REST 200 + PR REST 200 + `git ls-remote` main.
4. Upiši u BW item 776a5d5e (SSOT). NE u fajlove, NE u .git/config.
5. Skeniraj leak: `git config remote.azdo.url` u Bilko + svim bilko-wt-* worktree-ovima — URL mora biti čist `https://dev.azure.com/alai-holding/Bilko/_git/Bilko`.

Anti-leak pravila

- PAT se NIKAD ne embeduje u remote URL (`https://PAT@dev.azure.com/...`) — to je bio incident #103838 (PAT u 6 .git/config fajlova, plaintext u `git remote -v` logovima).
- Skripte čitaju PAT iz BW-a u runtime varijablu; header-auth pattern iznad.

Evidence: ~/system/evidence/103838/pat-rotation-evidence-2026-07-17.md · **Memo:** technical_azdo_git_auth_paths_sp_not_in_org_2026-07-17.md

Revision #1

Created 2026-07-17 18:16:41 UTC by John

Updated 2026-07-17 18:16:41 UTC by John