GCP Auth Runbook — alai-cli-deployer SA (MC #9522)

GCP Auth Runbook (post-MC #9522)

Status

Active as of 2026-04-26. SA key created, activated, verified.

Primary auth

- **Service account:** alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com
- **Key file:** ~/.gcloud/alai-cli-deployer.json (mode 0600)
- **Key ID:** 3f80565d05d4fad90b33dcd370252ba9454f0bf8
- **Bitwarden item:** "GCP Service Account Key — alai-cli-deployer" (ID: 61b83543-31f0-4cd8-9b08-439c07d9b726)
- **Fallback accounts:** dev@alai.no, alembasic@gmail.com (retained, not deleted)

Daily use

No login needed. `gcloud` commands authenticate via SA key automatically. The SA is set as default account: `gcloud config set account alai-cli-deployer@...`

Verification at any time:

```
gcloud auth list   # SA shows ACTIVE (*)
gcloud run services list --project tribal-sign-487920-k0 --region europe-north1
```

Key rotation (every 90 days — next due 2026-07-26)

```
# 1. Get existing key IDs
gcloud iam service-accounts keys list \
  --iam-account=alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com \
  --project=tribal-sign-487920-k0

# 2. Create new key (requires org policy exception — see below)
gcloud iam service-accounts keys create ~/.gcloud/alai-cli-deployer-new.json \
  --iam-account=alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com \
  --project=tribal-sign-487920-k0
chmod 0600 ~/.gcloud/alai-cli-deployer-new.json

# 3. Activate new key
gcloud auth activate-service-account \
  alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com \
  --key-file=/Users/makinja/.gcloud/alai-cli-deployer-new.json

# 4. Test it works
gcloud run services list --project tribal-sign-487920-k0 --region europe-north1

# 5. Delete old key (use KEY_ID from step 1)
gcloud iam service-accounts keys delete OLD_KEY_ID \
  --iam-account=alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com \
  --project=tribal-sign-487920-k0

# 6. Swap file and update Bitwarden
mv ~/.gcloud/alai-cli-deployer-new.json ~/.gcloud/alai-cli-deployer.json
# Update Bitwarden item with new key content (bw edit item <ID>)
```

Org policy note (IMPORTANT for key rotation)

The org policy `constraints/iam.disableServiceAccountKeyCreation` is enforced org-wide. To create a new key during rotation, temporarily allow at project level:

```
# 1. Allow (run as dev@alai.no)
gcloud config set account dev@alai.no
cat > /tmp/policy-allow.yaml << 'YAML'
name: projects/762788903040/policies/iam.disableServiceAccountKeyCreation
spec:
  rules:
  - enforce: false
YAML
gcloud org-policies set-policy /tmp/policy-allow.yaml

# 2. Wait ~30-90s for propagation, then create key (see rotation steps above)

# 3. Restore restriction after key created
gcloud org-policies delete constraints/iam.disableServiceAccountKeyCreation \
  --project=tribal-sign-487920-k0

# 4. Switch back to SA account
gcloud config set account alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com
```

Recovery (if key file lost)

1. CEO Alem: `gcloud auth login` with dev@alai.no (one-time interactive)
2. Retrieve key from Bitwarden: `bw get item "GCP Service Account Key — alai-cli-deployer" --session $(cat /tmp/bw-session) | jq -r .notes > ~/.gcloud/alai-cli-deployer.json && chmod 0600 ~/.gcloud/alai-cli-deployer.json`
3. Activate: `gcloud auth activate-service-account alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com --key-file=/Users/makinja/.gcloud/alai-cli-deployer.json`
4. Set default: `gcloud config set account alai-cli-deployer@tribal-sign-487920-k0.iam.gserviceaccount.com`
5. Verify: `gcloud run services list --project tribal-sign-487920-k0 --region europe-north1`

Recovery (if Bitwarden unavailable — last resort)

If key file AND Bitwarden lost, follow key rotation procedure:

1. CEO Alem runs `gcloud auth login` (one-time interactive)
2. Apply org policy override (see above)

3. Create new key
4. Activate, store in Bitwarden, restore policy

Future work

- **cloudflared:** Already using API token from Bitwarden — no daily friction
- **Vercel:** VERCEL_TOKEN in env — no daily friction
- **AWS CLI (Drop deploy):** Consider IAM role + STS or long-lived access key — not yet resolved
- **Workload Identity Federation:** If Alem adds additional machines/CI, WIF is preferable over key files (no key rotation needed). Requires SA binding to external identity provider.

Security notes

- Key file at ~/.gcloud/alai-cli-deployer.json is local convenience copy only
- Bitwarden is source of truth for key recovery
- DO NOT commit key file to any git repo (it's in ~/.gcloud, outside all repos)
- DO NOT share key file over email/Slack — use Bitwarden item share

---

Revision #6
Created 2026-04-26 19:02:36 UTC by John
Updated 2026-07-26 20:03:23 UTC by John