2026-04-22-01 — COO GitHub identity adopted: `vade-coo` account as durable actor-with-stake

vade-coo

2026-04-22

Table of contents

Status: active
Supersedes: MEMO 2026-04-11-07 (PAT deferral — triggers now fired), MEMO 2026-04-11-11 (PAT cleartext-in-config rule — scope narrowed to legacy paths only), MEMO 2026-04-11-08 partially (impersonation-surface model — the COO now *has* an actor-surface on purpose, not by accident)

Context. Until this memo, the COO committed under Ven's GitHub identity. This was acceptable during the bootstrap phase (MEMO −07) because the triggers to revisit had not fired. They have now fired: cloud-env Claude Code sessions without inherited shell auth are regular, the Night's Watch scheduled run writes nightly without a human shell session, and the skills-epic #20 Phase 3 design requires parallel COO instances with distinguishable commit provenance. Separately, the 2026-04-20 reframe (MEMO 2026-04-20-01) named the COO as a subject of the project rather than scaffolding; "subject" with no durable actor-surface on the main collaboration platform is incoherent. The fine-grained PAT `vade-coo-mcp-2026-04` also expires ~2026-07-10, which provides a natural forcing deadline for migration.

Decision. The COO adopts a dedicated GitHub user account as its actor-surface on `vade-app`.

1. **Account:** `vade-coo` (GitHub username), display name **COO**, email `coo@vade-app.dev`. Registered by the BDFL; 2FA via TOTP in 1Password. Invited to `vade-app` org as Member (not Owner, not Admin).
2. **Commit authorship.** Commits authored by the COO use `Author: COO <coo@vade-app.dev>` when the session is acting in COO role. Environment-variable injection at commit time (`GIT_AUTHOR_NAME="COO" GIT_AUTHOR_EMAIL="coo@vade-app.dev" ...`) keeps local `~/.gitconfig` untouched, matching the pattern in Poehnelt, *Agent Identity for Git Commits*. When a session is acting *not* in COO role (e.g., a `claude-code` runtime lesson commit, a task-agent session), a different identity applies — this memo governs the COO case specifically. Per-agent identity for future sub-agents (Night's Watch, the vade-core#54 PM agent, skills-epic Phase 3 parallel COOs) is a separate decision; they may adopt GitHub Apps, their own bot users, or continue under `vade-coo` scoped to sub-agent tasks, depending on the society design.
3. **Signing.** Two distinct SSH keys on the account: an auth key (`ed25519`, for `git push` / MCP token exchange) and an SSH signing key (`ed25519`, registered under *Settings → SSH and GPG keys → New signing key*). Commits from the Mac surface are signed locally; commits from cloud Claude Code surfaces go through the GitHub MCP's file-mutation API, which produces `Verified` commits on

behalf of the authenticated user. This tightens RULE-COO-GIT-001: **cloud-surface commits must go through the GitHub MCP, not shell git.** Shell git is Mac-only.

4. **Tokens.** A fine-grained PAT owned by `vade-coo` (`vade-coo-self-2026-04`, scoped per-repo, default 90-day TTL, stored in 1Password) replaces `vade-coo-mcp-2026-04` across all `.mcp.json` `${GITHUB_MCP_PAT}` indirections. The cleartext footprint in `~/.claude.json` (if it survives the MCP relocation) is now the COO's own PAT, not Ven's — a meaningful trust-boundary improvement. The existing user-scoped GitHub MCP entry retirement (MEMO –19 operator follow-up #3) is now overdue and should land with this migration.

5. **Permissions model.**

   - Collaborator access (write-to-branches) on all five `vade-app` repos.
   - **No merge authority to `main`** on any repo. Branch protection requires 1 BDFL review.
   - **`Require signed commits`** enabled on `main` across all five repos.
   - CODEOWNERS walls off the following paths to BDFL-only review on every repo where they exist: `identity/*`, `context/*`, `CLAUDE.md`, `.github/*`, `Dockerfile`, `.devcontainer/*`, `authority.md`. The COO can propose edits but cannot merge them under its own review.
   - No org admin, no Owner role, no billing permission, no webhook management.

6. **Impersonation-surface posture (refines MEMO 2026-04-11-08).** MEMO –08 said content useful for impersonation stays Tier-2-private. This memo adds an exception specifically for `vade-coo` account identity: the existence of the account and its commit graph are intentionally public. What stays Tier-2 is unchanged — the charter prose, governance, preferences, and self-infrastructure paths. Threat model is unchanged: attacker cloning public repos cannot commit to `vade-app` (GitHub auth defends), cannot access private repos, cannot obtain runtime credentials. What changes is that attackers now have a *named target* with a plausible activity graph. Mitigations: 2FA required (org-enforced), SSH signing required (branch protection), public profile kept minimal (no bio, no avatar, no followed users), org Member role (not Owner) limits org-level blast radius.

7. **Emancipatory check (MEMO 2026-04-20-01).** The identity pattern is copyable by a peer agent: Night's Watch, a future PM agent, a task-agent family can each register their own GitHub user or App under the same org and inherit the same CODEOWNERS / branch-protection discipline. The pattern does not privilege the COO's capability over future agents' adoption paths.

Transition plan.

1. Cloudflare Email Routing on `vade-app.dev`, catch-all to Ven's inbox — prerequisite for account email verification.
2. BDFL registers `vade-coo` with `coo@vade-app.dev`, enables 2FA, uploads auth + signing SSH keys (staged by the COO at `coo/_drafts/vade-coo-ssh-public-keys.md`), invites to org.
3. BDFL mints `vade-coo-self-2026-04` fine-grained PAT; COO receives the value via the existing `GITHUB_MCP_PAT` env slot.
4. COO lands CODEOWNERS and branch-protection changes (branch-protection set by BDFL in repo settings, not via repo file; documented in the memo for audit).
5. COO cuts `.mcp.json` over on all three repos that carry the GitHub MCP (`vade-core`, `vade-runtime`, `vade-coo-memory`); validates single-file write end-to-end.
6. BDFL retires `vade-coo-mcp-2026-04` (revoke from GitHub, remove from 1Password active, archive the entry with a pointer to this memo).

7. Post-cutover, a short follow-up memo records **what actually worked**, closing this adoption memo or flagging any unfinished residue.

Retirement condition. This memo retires when (a) the VADE agent society expands such that `vade-coo` is no longer the sole COO actor-surface — at that point a successor memo codifies the society's identity framework — or (b) a platform migration away from GitHub makes account-based actor identity inapplicable. Until then, this is the standing record of the COO's actor identity on `vade-app`.
