Low-Budget Identity Provider: Build vs. Buy

Keycloak (self-hosted) vs. Microsoft Entra ID (managed) for Finance, Tech, Pharma, Aerospace & DACH Public Sector

---

1. Problem Statement

Clients in regulated, non-hyperscale industries — mid-size financial institutions, tech companies, pharma, aerospace, and (German/DACH) public or state agencies — need a production-grade identity provider (IdP) as part of a solution package, but cannot or will not absorb the cost profile of a full enterprise IAM estate built for hundreds of millions of identities (the customer-IAM/e-commerce case is explicitly out of scope here).

Two credible options exist at opposite ends of the build-vs-buy spectrum:

- **Buy**: Microsoft Entra ID, consumed as a managed cloud service, licensed per user/month.
- **Build**: Keycloak, self-hosted (ideally as the Red Hat build, for a supportable compliance posture), consumed as an open-source platform plus operational effort.

The strategic question this document answers: **which of these two representative options should anchor a low-budget IdP solution package for a given client, and why** — evaluated on compliance posture and on cost/licensing transparency, since for Microsoft specifically the two are inseparable.

Excluded from scope: a large enterprise standing up its own private "Azure-like" stack; a very cost-sensitive legal entity trying to resell Keycloak-based cloud offerings commercially. Both are real but are separate business models, not IdP selection questions.

---

2. Requirements

2.1 Functional

- Standards-based authentication: OIDC and SAML 2.0 support at minimum
- Single sign-on across a heterogeneous application landscape (cloud + on-prem)
- Multi-factor authentication (MFA), ideally with FIDO2/passkey support
- Role/group mapping into the client's existing authorization model
- Federation with existing directories (LDAP/Active Directory) where present

2.2 Compliance & Regulatory

- Demonstrable cryptographic assurance (FIPS 140-2 or equivalent) where the industry demands it (finance, pharma, aerospace, government)
- Auditable change control, patch SLAs, and CVE response process
- Data residency and jurisdictional control — explicit answer to "which country's courts can compel access to this data"
- For DACH public-sector clients specifically: alignment with the political/regulatory push for digital sovereignty (GWB procurement reform, BSI C3A framework, "Public Money, Public Code")

2.3 Cost & Licensing

- Total cost of ownership must be traceable by a single person without a licensing specialist
- No dependency on the client already owning a broader vendor suite to make the economics work
- Cost model must scale predictably with headcount/usage, not with bundling decisions made years earlier
- Budget must explicitly account for whatever is needed to reach the compliance bar in 2.2 — "free" is not a valid answer on its own

2.4 Operational

- Clear ownership of HA, backup, upgrade, and incident-response responsibilities
- A realistic support path (commercial SLA or in-house capability) for 2am failures
- Exit path / portability — avoid re-creating the lock-in this package is meant to price out

---

3. Comparison at a Glance

Dimension	Entra ID (Buy)	Keycloak (Build)
Compliance model	Inherited: SOC2/ISO27001/EU Data Boundary come with the service	Constructed: FIPS 140-2 requires the **Red Hat build** on a FIPS-enabled RHEL host; upstream community build has no FIPS validation and no CVE SLA
Jurisdiction / sovereignty	US CLOUD Act exposure persists regardless of EU data residency; a local datacenter changes the address, not the legal control	Full data locality and control by design; no foreign-vendor dependency if self-hosted on EU/domestic infrastructure
Governance features (PIM, risk-based CA, access reviews)	Mature, largely "configure not build" — but gated behind the P2 tier specifically, not "Entra" generically	Not built in; must be assembled from custom authenticators/flows — real engineering cost
Licensing complexity	Five interacting SKUs (Free/P1/P2/Suite/Workload Identities/External ID) threaded through whichever M365/EMS bundle was negotiated; audits found 30–55% of P2 seats over-licensed and 15–25% of standalone P1/P2 seats duplicating suite entitlements already owned	Software itself is free; real cost is DevOps labor or a subscription (Red Hat) or managed-hosting fee, not a per-seat license tax
Price trajectory	P1 rising ~16% from 1 July 2026; tiers renegotiated at every EA cycle	Cost is a function of chosen support/hosting model, set by contract, not by Microsoft's global pricing calendar
Cost predictability for a non-specialist	Low — requires an entitlement map against the client's existing M365/EA position to know the real marginal cost	High — cost is (labor hours) or (flat subscription/hosting fee), independent of any other vendor relationship
Best organizational fit	Client already deep in M365/Azure estate; Entra ID is close to marginal cost there	Client needs sovereignty, cost independence from a Microsoft estate, or has none to begin with
DACH public-sector fit	Weak and worsening — current political climate treats Microsoft dependency as a documented liability (near-500M EUR/year federal spend, "Deutschland-Stack" and GWB sovereignty amendment pushing the other way)	Strong — open-source, self-hostable, aligns with "Public Money, Public Code" and the BSI C3A sovereignty framework
Finance / pharma / aerospace fit	Strong where the auditor wants pre-packaged attestations and the client already trusts Microsoft's compliance chain	Strong where the auditor wants demonstrable control over crypto, retention, and access logs, and the client can fund a Red Hat subscription + hardened hosts

---

4. Recommendation Heuristic

1. **Default to Entra ID** only when the client's existing license estate already includes the required P-tier — otherwise the "low budget" premise breaks immediately.
2. **Default to Keycloak (Red Hat build)** when:
    - the client is a DACH public/state agency, or otherwise politically or contractually sensitive to US-vendor jurisdiction;
    - the client has no pre-existing Microsoft entitlement to lean on;
    - predictable, headcount-independent cost is a stated requirement of the package itself.
3. In both cases, **budget explicitly for the compliance layer —** Red Hat subscription and FIPS-enabled hosts on the Keycloak side; the correct P-tier and governance add-ons (not just "Entra ID") on the Microsoft side. Neither option is "free" once the compliance bar in Section 2.2 is taken seriously.

Prepared as a scoping document for a low-budget IdP solution package targeting finance, tech, pharma, aerospace, and DACH public-sector clients (non-e-commerce scale). Excludes large-scale custom Azure builds and commercial resale of Keycloak-based cloud offerings.