

IDENTITY ARCHITECTURE LEDGER (IAL)

Immutable cryptographic baseline recording for the AI and Cloud Pipeline Hardening Framework (ACPHF).

Deployment Target: GitHub Actions CI/CD	Target Cloud: Microsoft Azure
Execution Date: 2026-08-10	Ledger State: [VERIFIED - AUDIT READY]

[SECTION 1: CORE CLOUD BOUNDARY IDENTIFICATION]

1.1 Deterministic Routing Coordinates

Anchoring the globally unique root coordinates via active CLI discovery commands.

Tenant ID (Identity Root): 8a1b2c3d-4e5f-6g7h-8i9j-0k1l2m3n4o5p

Subscription ID (Asset Root): c2b1a3d4-e5f6-7g8h-9i0j-1k2l3m4n5o6p

1.2 Target Asset Configuration Profile

Provisioned Resource Name: kv-acphf-prod-eus-01

Resource Group Perimeter: rg-identity-security-prod

HARD BOOLEAN Workspace Path Cryptography

Are both the target subscription asset and the identity directory actively nested under the identical root tenant domain structure?

> [SUCCESS] Workspace paths align. CLI context locked.

[SECTION 2: NON-HUMAN IDENTITY PROVISIONING]

2.1 Identity Object Profile

Automated instantiation of the machine account and local execution context.

Application Name: acphf-agent-01

Application (Client) ID: d7e8f9a0-b1c2-d3e4-f5g6-h7i8j9k0l1m2

2.2 Architectural Attack Surface Minimization

- Single-Tenant Enforced: (AzureADMyOrg) Blocks external credential instantiation.
- Headless Execution (Blank Redirect URI): Denies interactive browser callback vectors.

HARD BOOLEAN Object Instantiation State

Has the programmatic execution successfully initialized both the central Application Object and the local enterprise Service Principal?

```
| > [SUCCESS] Blueprint and local security context created.
```

[SECTION 3: PASSWORDLESS CRYPTOGRAPHIC FEDERATION]

3.1 Federated Trust Parameters

Issuer URL: `https://token.actions.githubusercontent.com`

Audience Mapping: `api://AzureADTokenExchange`

3.2 Immutable Subject Claim Mapping

Explicit, case-sensitive string configuration for inbound OIDC handshakes.

```
Subject (sub): repo:[Target_Org]/[Target_Repo]:ref:refs/heads/[Target_Branch]
Applied State: repo:Compcode1/machine-identity-1:ref:refs/heads/main
```

- Subject claim contains zero production wildcards (*).
- Exact string casing verified to prevent AADSTS700213 drops.

HARD BOOLEAN Policy Enforcement

Has the cryptographic JSON payload been successfully written into the federated identity collection?

```
| > [SUCCESS] Trust policy active. Token endpoint listening.
```

[SECTION 4: DATA-PLANE ACCESS & PIPELINE ENFORCEMENT]

4.1 Role-Based Access Control (RBAC) Entitlements

Bypassing infrastructure control planes in favor of strict data-plane isolation.

Assigned Data-Plane Role: `Key Vault Secrets User`

`/subscriptions/c2b1a3d4-e5f6.../resourceGroups/rg-identity-security-prod/providers/Microsoft.KeyVault/vaults/kv-acphf-prod-eus-01`

Target Asset ID Scope:

4.2 Token Volatility & Secret Masking

- Access Token ceiling restricted to 60-minutes.
- Script-level runtime masking (::add-mask::) actively intercepting memory variables.

