IA

Microsoft CERTIFIED
IDENTITY AND ACCESS ADMINISTRATOR
ASSOCIATE

THE LEGACY STATE

The unmanaged baseline plagued by static secret sprawl, over-privileged service principals, and unmonitored pathways.

CONFIGURATION ENGINE & IDENTITY ARCHITECTURE LEDGER

The 4-phase ACPHF establishes a secure, zero-trust bedrock and strictly records all hard boolean validation states and RBAC assignments.

VERIFICATION & AUDIT RESULTS LEDGER

Active KQL diagnostics verify the mandatory gates (Coordinate, Character, Clock, Plane) and record telemetry outcomes as cryptographic proof.

CONTINUOUS ENTERPRISE ENVIRONMENT

ENTERPRISE NEEDS & CAPABILITY EXPANSION

Safely integrating the 35 Microsoft Entra ecosystem capabilities based on continuous and evolving business requirements.

ADAPTIVE LOOP

FINAL CONFIGURATION PACKAGE

An immutable, heavily audited core seamlessly combined with precise, adaptive modular security toolsets.

FIELD MANUAL

> Intelligent Architecture Enterprise Configurations & Documentation

01 | THE LEGACY STATE

The Input: The unmanaged enterprise baseline, heavily plagued by static secret sprawl, over-privileged service principals, and unmonitored legacy execution pathways.

02 | CONFIGURATION ENGINE & IAL

The Engine: The 4-phase ACPHF establishes a secure, zero-trust bedrock. The *Identity Architecture Ledger (IAL)* strictly records all hard boolean validation states, coordinates, and RBAC assignments.

03 | VERIFICATION & THE ARL

The Auditing: Active KQL diagnostics verify the 4 mandatory gates (Coordinate, Character, Clock, Plane). The *Audit Results Ledger (ARL)* records the telemetry outcomes as a cryptographic proof-of-governance receipt.

04 | MODULAR CAPABILITY EXPANSION

The Scale: With the core securely configured, recorded, and audited, the architecture safely scales by integrating the 35 Microsoft Entra ecosystem capabilities based strictly on business requirements.

05 | FINAL CONFIGURATION PACKAGE

The Output: A tailored, fully proven enterprise architecture. It guarantees an immutable, heavily audited zero-trust core seamlessly combined with the precise modular security toolsets required for the deployment.

EXECUTIVE PREFACE: STRATEGIC IMPERATIVE & THREAT BASELINE

> Quantifying the Systemic Failure of Legacy Machine Credentialing

INDUSTRY VULNERABILITY BASELINE

99%

The Permission Gap

Industry telemetry confirms that 99% of cloud users, roles, and machine identities hold excessive, unused permissions, maximizing the blast radius.

Source: Palo Alto Networks Unit 42 Cloud Threat Report

44%

The Breach Reality

44% of enterprise organizations have experienced a cloud breach, with credential compromise and unmanaged access serving as the dominant threat vectors.

Source: Thales Global Cloud Security Study & Verizon DBIR

LEGACY ARCHITECTURE FLAWS

Static Secret Dependency

Relying on long-lived symmetric keys across CI/CD pipelines creates unmanageable attack surfaces. Manual rotation introduces operational friction and catastrophic exposure windows.

Subscription Blast Radius

Pre-modernization machine identities frequently hold overly broad administrative roles (e.g., Contributor) rather than zero-trust scoping, turning a single compromised agent into a subscription-wide breach.

Supply-Chain Vulnerability

Hardcoded credentials within repositories and build environments provide threat actors with direct, low-resistance vectors for lateral movement into core infrastructure.

ENTERPRISE FIELD MANUAL: ACTIVE ENGINEERING BASELINE

> Command-Line Interface (CLI) Execution Protocol for Microsoft Entra ID

PART 1: The ACPHF Core Engineering Specification

The architectural blueprint for identity fleet management. Details the 4-phase CLI execution (Boundary, Provisioning, Federation, Access) required to establish passwordless OpenID Connect (OIDC) federation and dynamic data-plane RBAC isolation.

PART 2: Identity Architecture Ledger (IAL)

The standardized configuration artifact. Captures immutable CLI baseline records for single-tenant schemas, headless service principals, and user-created managed identities to guarantee zero-trust alignment prior to runtime execution.

PART 3: Practical Log Navigation & Audit Guide

The operational telemetry runbook. Leverages Azure Log Analytics and KQL to visually audit inbound OIDC handshakes, trace downstream requests, and hunt for "Silent 403" authorization drops.

PART 4: Audit Results Ledger (ARL)

The proof-of-governance artifact. Structures KQL telemetry outcomes to rigorously verify the four mandatory architectural gates (Coordinates, Characters, Clock, and Plane) for continuous compliance.

PHASE 1: CORE CLOUD BOUNDARY & METADATA ALIGNMENT

> Establishing Deterministic Routing Coordinates

ARCHITECTURAL RATIONALE

Identity Root Boundary

Target: Microsoft Entra ID (Root Identity Authority).
Isolates the central security directory coordinating all identity operations.

Infrastructure Resource Boundary

Target: Azure Resource Scope (Target Asset Environment).
Locks down the explicit infrastructure perimeter containing the target workload assets.

Execution Lock

Before issuing tokens or assigning RBAC roles, the programmatic execution environment must be explicitly hard-locked to the exact Entra ID Tenant and Azure Subscription coordinates, neutralizing cross-tenant routing vulnerabilities.

CLI EXECUTION: BOUNDARY_CONTEXT.SH

```
# Phase 1: Deterministic Boundary Resolution
# Explicitly set execution context to prevent cross-tenant leaks

# 1. Target Identity Root (Microsoft Entra ID Tenant)
az login --tenant "<Target_Tenant_ID>"

# 2. Lock Infrastructure Scope (Azure Subscription)
az account set --subscription "<Target_Subscription_ID>"

# 3. Verify Active Boundary Matrix
az account show \
  --query "{Tenant:tenantId, Subscription:id}" \
  --output table
```

PHASE 2: NON-HUMAN IDENTITY PROVISIONING

> Directory Schema Creation & Attack Surface Minimization

ARCHITECTURAL RATIONALE

Global Application Blueprint

Target: Directory Schema.
Establishes the core identity schema and instantiates the local enterprise Service Principal context required for RBAC assignment.

Tenancy Boundary Enforcement

Target: Single-Tenant (AzureADMyOrg).
Locks authentication strictly within the internal home directory, preventing external multi-tenant credential instantiation.

Attack Surface Minimization

Target: Headless Execution.
Explicitly omits Redirect URIs to strip away interactive login vectors and deny browser callbacks at inception.

CLI EXECUTION: PROVISION_IDENTITY.SH

```
# 1. Register Headless Application Blueprint
# Enforces Single-Tenant boundary. Omitting reply-uris
# inherently denies browser callbacks.
APP_ID=$(az ad app create \
  --display-name "acphf-agent-01" \
  --sign-in-audience "AzureADMyOrg" \
  --query appId -o tsv)

# 2. Instantiate Local Security Context
az ad sp create --id $APP_ID

# 3. Verify Attack Surface Minimization
az ad app show --id $APP_ID \
  --query "{Audience:signInAudience,
WebRedirects:web.redirectUris}"
```

PHASE 3: PASSWORDLESS CRYPTOGRAPHIC FEDERATION

> OIDC Trust Establishment, Immutable Mapping & Validation Gates

ARCHITECTURAL RATIONALE

Subject Claim Guard (Invariants)

Target: Immutable DB ID (@<Immutable_DB_ID>).
Enforces absolute case-sensitive matching and zero-wildcard boundaries to eliminate AADSTS700213 mismatch errors and repository renaming attacks.

Ephemeral Token Exchange

Target: 60-Min Access Token Ceiling.
Translates the external JWT into a strictly scoped Entra ID Access Token. Forces continuous runtime re-authentication with zero static secrets provisioned.

CLI EXECUTION & JSON PAYLOAD

```
// 1. Immutable Claim Mapping Payload (fic_parameters.json)
{
  "name": "<Agent_Name>-github-oidc",
  "issuer": "https://token.actions.githubusercontent.com",
  "subject": "repo:
<Org_Name>/<Repo_Name>@<Immutable_DB_ID>:ref:refs/heads/<Target_Branch>",
  "audiences": ["api://AzureADTokenExchange"]
}

# 2. Programmatic FIC Enforcement (Azure CLI)
az ad app federated-credential create \
  --id $APP_ID \
  --parameters @fic_parameters.json
```

PHASE 4: DATA-PLANE ACCESS CONTROL & PIPELINE EXECUTION

> Isolation Roles, OIDC Handshake Orchestration & Telemetry Leak Prevention

ARCHITECTURAL RATIONALE

Plane Isolation (Control vs. Data)

Target: Least-Privilege Assignment.
Bypasses broad infrastructure management roles (e.g., Contributor) in favor of scoped data-plane authorizations (e.g., Key Vault Secrets User) applied directly to the Service Principal.

Session Lifecycle Hardening

Target: Volatile Token Rule.
Enforces a strictly volatile 60-minute access token ceiling. No long-lived refresh tokens are provisioned; pipelines must re-authenticate per run.

Telemetry Masking

Target: Runtime Leak Prevention.
Automated scanners fail to catch raw dynamic outputs. Script-level suppression commands intercept and redact variables in memory before plaintext logging.

CLI EXECUTION & HARDENING

```
# 1. Dynamically Fetch Target Resource ID
RESOURCE_ID=$(az resource show --name "<Target_Asset_Name>" \
  --resource-type "<Asset_Type>" --query id -o tsv)

# 2. Assign Least-Privilege Data-Plane Role
az role assignment create \
  --assignee-object-id $SP_OBJECT_ID \
  --assignee-principal-type "ServicePrincipal" \
  --role "<Data_Plane_Role_Name>" \
  --scope $RESOURCE_ID

# 3. Pipeline Runtime Masking Directive
echo "::add-mask::${{ secrets.<DYNAMIC_PAYLOAD_VAR> }}"
```

CONTINUOUS GOVERNANCE: IDENTITY ARCHITECTURE LEDGER

> Configuration Baseline Recording & Framework State Mapping

ARCHITECTURAL RATIONALE

Immutable Baseline Mapping

Target: Audit-Ready Configuration States.
The Identity Architecture Ledger (IAL) serves as the master artifact, capturing exact hard boolean validation states, directory GUIDs, and specific RBAC assignments to create an immutable architectural record.

Automated AI/Agent Ingestion

Target: Programmatic Compliance.
The ledger format is optimized for AI ingestion, allowing continuous operational execution and real-time framework alignment checks rather than manual portal reviews.

Structured Execution Enforcement

Target: Framework Phase Alignment.
Each phase of the pipeline hardening framework directly populates a distinct ledger section, translating engineering tasks into verifiable governance artifacts.

MASTER CONFIGURATION STATE FILE

```
# IDENTITY ARCHITECTURE LEDGER (IAL) STATUS MATRIX
# AI-INGESTION FORMAT v2.4

TARGET_CLOUD_ENV: AZURE_COMMERCIAL
AUDIT_STATE:      VERIFIED

------------------------------------------------------------
[1] CORE STRUCTURAL BOUNDARY DISCOVERY
IAL SECTION 1: Boundary Identification ........ [LOCKED]
  > TGT_SUB_ID, SRC_TENANT_ID Matched

[2] NON-HUMAN IDENTITY PROVISIONING
IAL SECTION 2: Identity Provisioning .......... [LOCKED]
  > Single-Tenant Enforced, Headless Verified

[3] CRYPTOGRAPHIC FEDERATION (OIDC)
IAL SECTION 3: Federated Credential State ..... [VALIDATED]
  > Subject Claim Mapped, Wildcards Blocked
```

CONTINUOUS GOVERNANCE: PRACTICAL LOG NAVIGATION

> Telemetry Auditing, Circuit Execution & KQL Diagnostics

ARCHITECTURAL RATIONALE

Dual-Interface Auditing

Target: End-to-End Verification.
Auditing requires two core interfaces: The Entra ID Sign-In Logs to verify the initial OIDC cryptographic handshake, and Azure Log Analytics (KQL) for deep-dive tracing of long-term trends and data-plane access.

Detecting the "Silent 403"

Target: Authorization Drops.
A successful directory login does not guarantee workload success. Telemetry must be parsed to detect drops where the identity authenticated successfully but lacked the specific data-plane RBAC required to extract the payload.

Complete Circuit Verification

Target: Operation Correlation.
Matches the token issuance at the Control Plane directly with a resulting `SecretGet (HTTP 200)` event on the target asset.

AZURE LOG ANALYTICS WORKSPACE (KQL)

```kql
// Gate 4: Data-Plane Access & Silent 403 Diagnostic
// Executes within active Log Analytics Workspace

KeyVaultRequests
| where TimeGenerated > ago(24h)
| where VaultName =~ "<Target_Vault_Name>"
| where IdentityCode == "<Service_Principal_ID>"
    or AppId == "<Application_ID>"
| project TimeGenerated, VaultName, OperationName,
          ResultSignature, HttpStatusCode, CallerIpAddress
| sort by TimeGenerated desc
```

CONTINUOUS GOVERNANCE: AUDIT RESULTS LEDGER (ARL)

> Cryptographic Traceability & The 4 Mandatory Validation Gates

ARCHITECTURAL RATIONALE

Proof of Governance

Target: End-to-End Compliance.
The ARL functions as the formal proof-of-governance verification report, mapping telemetry correlations and logging pass/fail outcomes for every automated pipeline execution.

Defect & Remediation Matrix

Target: Actionable Diagnostics.
Rather than hunting for random anomalies, the framework uses the 4 Gates to instantly diagnose root causes (e.g., mismatching character strings or expired token lifetimes) and assign direct remediation actions.

Human-AI Collaboration

Target: Runtime Validation.
The engineer provisions the cloud boundary while the AI agent dynamically evaluates the KQL telemetry against the ledger constraints to log a hard boolean success state.

THE 4 MANDATORY AUDIT GATES

1 COORDINATE CHECK
Validates that the external runner is utilizing the exact, matching `Tenant ID` and `Application ID` boundaries.

2 CHARACTER CHECK
Validates the exact string casing of the Subject Claim against the external repository to prevent `AADSTS700213` authentication drops.

3 CLOCK CHECK
Validates the `60-minute token volatility` ceiling, ensuring long-running pipelines execute a successful re-authentication loop.

4 PLANE CHECK
Validates the transition from the Control Plane to the Data Plane, confirming `SecretGet (HTTP 200)` execution with zero Silent 403 drops.

INDEX: SYSTEM SYNTHESIS & FOUNDATION

> Core Baseline Verified & Capability Deployment Readiness

ARCHITECTURAL RATIONALE

Zero-Trust Foundation

Target: Machine Identity Baseline.
By strictly enforcing the 4-phase ACPHF, all non-human identities now operate entirely without static secrets and are strictly confined to data-plane isolation boundaries.

Verified Governance

Target: Immutable Proof.
The Identity Architecture Ledger (IAL) and Audit Results Ledger (ARL) guarantee that the actively deployed environment perfectly matches the intended architectural design.

Ecosystem Readiness

Target: Control Plane Expansion.
With the foundational identity vulnerabilities neutralized and audited, the architecture is now fully prepared to safely integrate broader Microsoft Entra Control Plane capabilities.

SYSTEM EXECUTION STATE

```
# INITIATING FULL SYSTEM SYNTHESIS CHECK...

[SYSTEM CHECK] ACPHF Core Engineering Spec ..... [VERIFIED]
[SYSTEM CHECK] Passwordless OIDC Federation .... [VERIFIED]
[SYSTEM CHECK] IAL Configuration States ........ [LOCKED]
[SYSTEM CHECK] KQL Telemetry Circuit ........... [VERIFIED]
[SYSTEM CHECK] ARL Governance (4 Gates) ........ [PASSED]

============================================================
STATUS: ZERO-TRUST IDENTITY FOUNDATION ESTABLISHED
============================================================

> SYSTEM READY:
> INITIATE CONTROL PLANE CAPABILITY TAXONOMY DEPLOYMENT
> EXTRACTING 35 CORE SERVICES...
```

INDEX: THE 35 CORE SERVICES

> Microsoft Entra Control Plane Capability Taxonomy & Service Coverage Map

01 Directory Foundations & Admin Boundaries

- Tenant Configuration & Global Settings
- Built-In & Custom Roles (RBAC)
- Administrative Units (AUs)
- Directory Objects
- Custom Security Attributes (CSAs)
- Device Management

02 Zero Trust Access Control & Context Engines

- Conditional Access (CA) Engine
- CA Authentication Context
- Protected Actions
- Microsoft Entra ID Protection
- Global Secure Access (GSA / SSE)

03 Credential Security & Auth Infrastructure

- Authentication Methods
- MFA Settings & Registration Campaigns
- Self-Service Password Reset (SSPR)
- Entra Password Protection
- Windows Hello for Business (WHfB)
- Microsoft Entra Kerberos

04 External Identities & Multi-Tenant Gov

- External Collaboration Settings (B2B)
- Cross-Tenant Access Settings (XTAS)
- Cross-Tenant Synchronization (CTS)
- External IdP Federation

05 Application & Workload Identity Control

- App Registrations & Service Principals
- Managed Identities for Azure Resources
- Enterprise Applications Management
- Microsoft Entra Application Proxy
- Defender for Cloud Apps (MDCA) Proxy

06 Identity Governance & Privileged Elevation

- Privileged Identity Management (PIM)
- Entra Entitlement Management
- Access Reviews
- Lifecycle Workflows (LCW)
- Terms of Use (ToU)

07 Hybrid Identity & Telemetry Engines

- Hybrid Identity Engines (Connect Sync, Cloud Sync, Password Hash Sync, and PTA)
- Seamless Single Sign-On (SSO)
- Microsoft Entra Connect Health
- Monitoring & Log Analytics