Zero Trust Architecture Implementation Guide for VA Loan Guarantee (LGY)

# Executive Summary – With IAM & MPI Integration

Implementing Zero Trust Architecture (ZTA) for LGY requires not only identity-aware access and continuous verification but also precise coordination with VA’s authoritative identity and access infrastructure: IAM (e.g., Azure AD, PingFederate, IAM Identity Center) and MPI (Master Person Index). MPI provides identity resolution, while IAM governs authentication, role assignment, and access enforcement. Together, they form the foundation for ZTA’s identity perimeter—ensuring only authenticated, contextually validated users and services interact with sensitive LGY systems and data.

# 1. Core ZTA Principles in the LGY Context

|  |  |
| --- | --- |
| Principle | LGY Example |
| Never Trust, Always Verify | No implicit trust for VA staff or contractors accessing loan processing tools; all access is authenticated and authorized. |
| Least Privilege Access | Mortgage underwriters receive read-only access to case files unless explicitly assigned update rights. |
| Micro-Segmentation | LGY subsystems (e.g., eligibility check in AWS, Salesforce case management, Oracle claims logic) operate in isolated VPCs with granular firewall rules. |

# 2. Reference Architecture

Architecture diagram placeholder: ZTA LGY IAM+MPI Architecture.

# 3. Implementation Steps

1. Step 1: Define Identity Perimeters - Use Azure AD + MFA for VA internal users. Use PingFederate or Cognito for federating external loan servicers.
2. Step 2: Establish Policy Enforcement Points (PEPs) - API Gateway, Istio sidecars, OPA policies for real-time enforcement.
3. Step 3: Enable Least Privilege with RBAC/ABAC - IAM roles per function with JIT elevation.
4. Step 4: Apply Micro-Segmentation - VPC security groups, Transit Gateways, service meshes for isolated communication.
5. Step 5: Integrate Telemetry and Continuous Monitoring - Splunk, GuardDuty, Sentinel, CRISP dashboards.
6. Step 6: ZTA Pilot Rollout - Begin with low-risk, high-value apps like Salesforce and eligibility microservices.

# 4. Integration Enhancements for IAM and MPI

## IAM Integration (Azure AD + AWS IAM Identity Center)

- User SSO: VA employees authenticate via Azure AD (SAML/OIDC + MFA).  
- Federated Access: PingFederate bridges external contractors to AWS & Salesforce.  
- Scoped Roles: IAM Identity Center issues fine-grained roles.  
- Context Evaluation: Device health, location, and risk score evaluated at login time.

## MPI Integration (Master Person Index)

- Identity Resolution: MPI validates claimants using ICN, EDIPI, or VA File Number.  
- Salesforce ↔ MPI Sync: Salesforce uses Salesforce Connect to virtualize MPI queries.  
- Lambda-Based Verification: AWS Lambda calls MPI to cross-check submitted identity info.

# 5. Enhanced Secure Access Workflow

1. User signs in via Azure AD → receives SAML token.  
2. PingFederate (if external) federates and applies Conditional Access policy.  
3. IAM Identity Center issues scoped role (e.g., lgy.loan.intake.viewer).  
4. API Gateway intercepts request → forwards to Lambda Authorizer.  
5. Lambda queries MPI to verify ICN / fileNumber combination.  
6. Access granted if IAM role + MPI identity resolution successful.  
7. Events logged in Splunk → CRISP dashboard.

# 6. Policy Enforcement Points and Examples

- AWS API Gateway: OPA / Rego – Deny access unless MPI verification is complete.  
- Salesforce Flow: Role-based + attribute-based logic – Allow view-only access to underwriters outside VBA.  
- Kubernetes (EKS + Istio): ABAC + service mesh routing – Block east-west traffic unless both services share VCN + tag.  
- Oracle Access Layer: Conditional SQL logic via proxy service – Validate user access scope from IAM before SELECT on claims.

# 7. IAM + MPI Alignment with NIST SP 800-207

- Identity Provider: Azure AD / PingFederate / IAM Identity Center  
- PDP (Decision Point): OPA or Lambda authorizer at API Gateway  
- PEP (Enforcement): Kong Gateway, Istio, AWS API Gateway, Salesforce Flow Builder  
- Trust Evaluation: MPI identity verification, device health, IAM roles  
- Telemetry Feed: CRISP, Splunk, AWS CloudTrail, Azure Sentinel

# 8. Next Steps: IAM + MPI ZTA Enhancements

- Define IAM permission sets for LGY-specific operations (create/update/approve claims).  
- Publish a policy decision matrix mapping claim processing steps to MPI-validated identity tiers.  
- Implement periodic revalidation of stale MPI records during long-lived session workflows.  
- Red/Blue team simulate identity spoofing attempts to test IAM+MPI policy enforcement.

A diagram of a company

AI-generated content may be incorrect.