Service Mesh Implementation Guide

Summit Digital Solutions, Inc.

Document Version: 1.2

Effective Date: January 9, 2024

1. Purpose and Scope

1. This Service Mesh Implementation Guide ("Guide") establishes the mandatory procedures and requirements for implementing service mesh architecture within Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform and client environments.

2. This Guide applies to all Company employees, contractors, and authorized third parties involved in service mesh implementation, maintenance, or operation.

2. Definitions

1. "Service Mesh" means a dedicated infrastructure layer for facilitating service-to-service communications between microservices using a proxy-based mesh network.

2. "Control Plane" means the centralized management layer that configures and controls the behavior of the data plane proxies.

3. "Data Plane" means the operational layer consisting of service proxies that mediate and control network communication between services.

4. "Peak Performance Platform" means the Company's proprietary digital transformation platform as described in Document Reference PP-2023-001.

3. Implementation Requirements

1. Architecture Standards

a) All service mesh implementations must utilize Company-approved proxy technology

b) Mesh topology must conform to zero-trust security architecture

c) Implementation must support both Kubernetes and virtual machine deployments

d) Control plane redundancy requirements per Section 5.2 must be met

2. Security Controls

a) All service-to-service communication must be encrypted using TLS 1.3 or higher

b) Authentication must use mutual TLS (mTLS) with automatic certificate rotation

c) Access policies must be defined using declarative configuration

d) Security logging requirements detailed in Section 6.3 must be implemented

3. Observability Requirements

a) Distributed tracing integration is mandatory

b) Metrics collection must include latency, traffic, errors, and saturation

c) Logging must be configured for both control and data plane components

d) Integration with Company's central monitoring platform is required

4. Implementation Procedures

1. Pre-Implementation Phase

a) Complete architecture review and approval process

b) Document service dependency mapping

c) Establish performance baselines

d) Create rollback plan

e) Obtain security team sign-off

2. Implementation Phase

a) Deploy control plane components in high-availability configuration

b) Implement service proxy injection mechanism

c) Configure traffic management policies

d) Establish monitoring and alerting

e) Document as-built architecture

3. Validation Phase

a) Execute test suite per Test Protocol TP-2024-003

b) Verify security controls

c) Validate observability data

d) Perform load testing

e) Obtain operational readiness approval

5. Operational Requirements

1. High Availability

a) Control plane must maintain 99.99% availability

b) Automatic failover configuration is mandatory

c) Geographic distribution requirements per client SLA

d) Backup and recovery procedures must be documented and tested

2. Performance Standards

a) Maximum latency impact: 10ms per service hop

b) Memory overhead: Not to exceed 256MB per proxy instance

c) CPU utilization: Not to exceed 10% of host resources

d) Connection pool limits must be configured per service

6. Compliance and Governance

1. All implementations must comply with:

a) Company Information Security Policy (ISP-2023-001)

b) Data Protection Standards (DPS-2023-002)

c) Client-specific security requirements

d) Applicable regulatory requirements

2. Documentation Requirements

a) Architecture diagrams

b) Configuration specifications

c) Security controls documentation

d) Operational runbooks

e) Incident response procedures

7. Maintenance and Updates

1. Regular maintenance must include:

a) Monthly security patches

b) Quarterly version updates

c) Annual architecture review

d) Continuous configuration optimization

2. Change Management

a) All changes must follow Company change management procedures

b) Emergency change procedures per document ECM-2023-001

c) Version control requirements for configuration files

8. Legal Disclaimers

1. This document is confidential and proprietary to Summit Digital Solutions, Inc.

2. No part of this document may be reproduced or transmitted without express written permission.

3. The Company reserves the right to modify this Guide at any time.

9. Document Control

Document Owner: Chief Technology Officer

Last Review Date: January 9, 2024

Next Review Date: July 9, 2024

Document ID: SIG-2024-001

10. Approval

APPROVED BY:

Michael Chang

Chief Technology Officer

Summit Digital Solutions, Inc.

Date: January 9, 2024

James Henderson

Chief Digital Officer

Summit Digital Solutions, Inc.

Date: January 9, 2024