ATB vs Industrial Edge SPIFFE: A Comparative Analysis

Mauricio A. Fernandez F.

January 2026

Abstract

This document provides a comprehensive comparison between the Agent Trust Broker (ATB) architecture and the SC2 Industrial Edge SPIFFE implementation, analyzing their approaches to identity, authorization, and secure communication in distributed systems.

Contents

Executive Summary

Both ATB and SC2's Industrial Edge implementation leverage SPIFFE/SPIRE for workload identity, but they serve fundamentally different purposes and operate in distinct environments. This analysis examines their architectural differences, authorization models, and suitability for various use cases.

1. Identity Model Comparison

ATB Approach

ATB uses SPIFFE identities as the foundation for **AI agent authorization**:

```
spiffe://trust-domain/agent/<agent-type>/<instance>
```

Key characteristics: - Identity represents an AI agent workload - SVIDs are used to obtain Proof of Authorization (PoA) tokens - Identity is one layer in a multi-layer authorization system - Focus on **what the agent is allowed to do**, not just who it is

SC2 Industrial Edge Approach

SC2 uses SPIFFE identities for **device and workload authentication** in industrial settings:

```
spiffe://trust-domain/device/<device-type>/<location>
```

Key characteristics: - Identity represents physical devices, PLCs, or edge workloads - SVIDs are used directly for mTLS communication - Focus on **proving identity** for secure communication - Hierarchical trust based on physical topology

Key Difference

Aspect	ATB	SC2 Industrial Edge
Primary Subject	AI Agents	Industrial Devices
Identity Purpose	Authorization basis	Authentication
Trust Model	Capability-based	Location/device-based
Dynamic Scope	Per-request constraints	Static device permissions

2. Authorization Flow Comparison

ATB: Multi-Layer Authorization

```
Agent → AgentAuth → PoA Token → Broker → OPA Policy → Upstream API
```

1. Agent proves identity with SVID
2. AgentAuth issues scoped PoA token
3. Broker validates PoA and enforces policy
4. Each request carries fine-grained authorization

Advantages: - Dynamic, per-request authorization scoping - Human accountability chain preserved - Audit trail for every action - Constraints can change without re-attestation

SC2: Identity-Based Access Control

```
Device → SPIRE Agent → SVID → mTLS → Target Service
```

1. Device attests to SPIRE Agent
2. SVID proves device identity
3. Target service validates SVID
4. Access granted based on identity mapping

Advantages: - Simpler architecture - Lower latency (no token exchange) - Well-suited for static access patterns - Hardware attestation for physical security

3. Trust Anchor Comparison

ATB Trust Model

```
Human Operator
      ↓ (delegates)
Enterprise Policy
      ↓ (constrains)
PoA Token
      ↓ (authorizes)
Agent Action
```

- Trust originates from human accountability
- Policy defines allowable agent behaviors
- Every action traces back to an accountable party
- Legal and compliance requirements built-in

SC2 Trust Model

```
Root CA (SPIRE Server)
      ↓ (attests)
Intermediate CA (Nested SPIRE)
      ↓ (issues)
Workload SVID
      ↓ (authenticates)
Device/Service
```

- Trust originates from cryptographic chain
- Hardware attestation (TPM) provides root of trust
- Physical security of devices is paramount
- Hierarchical delegation through nested SPIRE

4. Attestation Methods

ATB Attestation

Method	Use Case
Kubernetes	Cloud-native AI workloads
AWS IID	EC2-based agents
GCP IIT	GCE-based agents
Azure MSI	Azure VM agents
Unix	Development/testing

Focus: Cloud workload attestation

SC2 Industrial Attestation

Method	Use Case
TPM DevID	Hardware-backed device identity
X509 Bootstrap	Legacy device migration
Join Token	Controlled provisioning
OIDC Federation	Cloud-to-edge bridging

Focus: Hardware and physical device attestation

5. Use Case Suitability

ATB Excels At

1. **AI Agent Orchestration** - Managing what autonomous agents can do
2. **Dynamic Authorization** - Changing permissions per request
3. **Audit Compliance** - Tracking actions to accountable parties
4. **API Gateway Protection** - Securing backend services from agents
5. **Multi-Tenant AI** - Isolating agent capabilities per tenant

SC2 Industrial Edge Excels At

1. **Device Authentication** - Proving device identity at scale
2. **OT/IT Convergence** - Bridging industrial and enterprise networks
3. **Edge Computing** - Securing distributed edge deployments
4. **Hardware Root of Trust** - TPM-backed identity
5. **Air-Gapped Networks** - Offline attestation support

6. Architectural Complexity

ATB Architecture

Components:

- AgentAuth Service
- Broker (API Gateway)
- OPA Policy Engine
- SPIRE (Identity)
- Audit Pipeline
- Key Management

Complexity: Higher - Multiple components for fine-grained control

Justification: AI agents require dynamic, auditable authorization that simple identity doesn't provide.

SC2 Architecture

Components:

- SPIRE Server (Root)
- SPIRE Server (Nested, per-site)
- SPIRE Agents (per-device)
- Workloads with Envoy/SDK

Complexity: Lower - SPIFFE-native with minimal additions

Justification: Industrial devices need reliable identity, not complex authorization logic.

7. Security Properties

Common Strengths

- Zero-trust network assumptions
- Cryptographic identity (X.509 SVIDs)
- Automatic credential rotation
- No static secrets in workloads

ATB-Specific Security

Property	Implementation
Least Privilege	Per-request PoA scoping
Human Accountability	Legal basis in every token
Action Audit	Complete audit trail
Policy Enforcement	OPA at gateway

SC2-Specific Security

Property	Implementation
Hardware Attestation	TPM DevID verification
Physical Security	Device location binding
Offline Operation	Pre-provisioned trust bundles
Network Segmentation	Per-site SPIRE servers

8. Operational Considerations

ATB Operations

Pros: - Kubernetes-native deployment - Cloud provider integrations - Centralized policy management - Observable audit pipeline

Cons: - More moving parts - Requires OPA expertise - Token management overhead - Higher latency per request

SC2 Operations

Pros: - Simpler SPIFFE-only deployment - Works in constrained environments - Lower operational overhead - Proven in industrial settings

Cons: - Less flexible authorization - Harder to audit at action level - Static permission model - Requires TPM infrastructure

9. When to Choose Each

Choose ATB When

- Deploying AI agents that access sensitive APIs
- Requiring human accountability for agent actions
- Needing dynamic, per-request authorization
- Operating in regulated environments (GDPR, SOX)
- Building multi-tenant AI platforms

Choose SC2 Industrial Edge When

- Securing industrial devices and PLCs
- Operating in OT environments
- Requiring hardware-backed identity (TPM)
- Working with constrained edge devices
- Bridging air-gapped networks

Hybrid Approach

Organizations with both AI agents and industrial edge can use:

```
Industrial Edge (SC2)     Cloud AI (ATB)
        ↓                       ↓
    Device SVID             Agent SVID
```

```
    ↓                      ↓
Edge Gateway  ←→    ATB Broker
    ↓                      ↓
OT Services         Enterprise APIs
```

The SC2 edge provides device identity, while ATB provides agent authorization for AI workloads accessing enterprise resources.

10. Conclusion

ATB and SC2's Industrial Edge SPIFFE implementation are complementary rather than competing solutions:

Aspect	ATB	SC2 Industrial Edge
Focus	AI Agent Authorization	Device Authentication
Environment	Cloud/Enterprise	Industrial/Edge
Authorization	Dynamic, per-request	Static, identity-based
Trust Root	Human Accountability	Hardware (TPM)
Complexity	Higher (more features)	Lower (focused scope)
Best For	AI orchestration	Device security

Recommendation: Use SC2 for industrial device identity at the edge, and ATB for AI agent authorization in the enterprise. The two can be bridged through federated SPIFFE trust domains.

Document prepared for architectural review and decision-making.