Frequently Asked Questions (FAQ)

General

What is ATB?

ATB (Agent Trust Broker) is a security gateway that controls what AI agents can do in enterprise environments. It ensures every agent action is authenticated, authorized, and audited.

Why do I need ATB?

When AI agents interact with enterprise systems (SAP, Salesforce, databases, etc.), you need: - **Access control**: Limit what agents can do - **Approval workflows**: Human oversight for sensitive actions - **Audit trails**: Know who did what and why - **Compliance**: Meet GDPR, SOX, and other regulations

How is ATB different from regular API gateways?

Feature	API Gateway	ATB
Authentication	API keys, OAuth	SPIFFE workload identity
Authorization	Role-based (RBAC)	Action-based with constraints
Approval flows	None	Built-in human-in-the-loop
Risk tiers	None	Low/Medium/High with escalation
Legal basis	None	Required for compliance
Dual control	None	Built-in for high-risk actions

What AI platforms work with ATB?

ATB is platform-agnostic. It works with: - OpenAI/GPT agents - Anthropic Claude - Microsoft Copilot - LangChain agents - Custom agent frameworks

The agent just needs to: 1. Obtain a SPIFFE identity 2. Request PoA tokens for actions 3. Include PoA tokens in requests

---

Architecture

What is a PoA token?

A Proof-of-Authorization (PoA) token is a signed JWT that authorizes a specific action. It includes: - **What**: The action being authorized (`act`) - **Who**: The agent's identity (`sub`) - **Limits**: Constraints on the action (`con`) - **Why**: Legal basis for the action (`leg`) - **When**: Expiration time (`exp`)

What is SPIFFE?

SPIFFE (Secure Production Identity Framework for Everyone) provides cryptographic identities for workloads. Instead of API keys or passwords, each service gets an X.509 certificate that proves its identity.

Do I need SPIRE to use ATB?

For production, yes. SPIRE provides: - Automatic certificate rotation - Workload attestation - Federation between trust domains

For development, you can use self-signed certificates.

What is OPA and why does ATB use it?

OPA (Open Policy Agent) is a policy engine. ATB uses OPA because: - Policies are code (version controlled, testable) - Decoupled from application logic - Industry standard for cloud-native authorization - Supports complex policy logic

---

Risk Tiers

How are risk tiers determined?

Risk tiers are defined in the OPA policy based on: - **Action type**: Payment execution vs. status read - **Data sensitivity**: PII access vs. public data - **Impact**: Irreversible changes vs. read-only queries

Can I customize risk tiers?

Yes! Edit `opa/policy/poa.rego`:

```
# Add a custom high-risk action
high_risk_actions["custom.dangerous.action"]

# Or change an existing action's tier
medium_risk_actions["sap.vendor.create"]  # Was high-risk
```

What happens if no risk tier matches?

Actions without a defined tier are denied by default. This is a security measure—explicit allow, implicit deny.

Can the same action have different risk tiers?

Yes, based on constraints. For example:

```
# Low amount = medium risk
risk_tier = "medium" {
  input.poa.act == "payment.execute"
  input.poa.con.amount <= 1000
}

# High amount = high risk
risk_tier = "high" {
  input.poa.act == "payment.execute"
  input.poa.con.amount > 1000
}
```

Approvals

How do approvals work?

1. Agent requests authorization for an action
2. If medium/high risk, a challenge is created
3. Approvers are notified (via your workflow system)
4. Approvers submit their approval
5. Once requirements are met, PoA token is issued

Who can be an approver?

Anyone with an `approver_id`. This is typically: - Email addresses - Employee IDs - SSO usernames

ATB doesn't authenticate approvers—that's your responsibility. Integrate with your existing identity provider.

What is dual control?

Dual control requires **two different people** to approve high-risk actions. This prevents: - Single point of compromise - Insider threats - Accidental approvals

Can the requester approve their own request?

No. The agent's identity (`sub`) cannot match any approver's ID.

How long do I have to approve?

Default is 5 minutes (`CHALLENGE_TTL_SECONDS=300`). After that, the challenge expires and must be recreated.

Security

Are PoA tokens encrypted?

PoA tokens are **signed** (to verify authenticity) but not encrypted. They're transmitted over mTLS, which provides encryption in transit.

If you need payload encryption, implement it at the application layer.

What prevents token replay?

Each token has a unique `jti` (JWT ID). The broker caches seen JTIs until they expire. Reusing a token returns `token_already_used`.

What if an agent's key is compromised?

1. Revoke the SPIFFE identity in SPIRE
2. Rotate the signing key in AgentAuth
3. All existing tokens become invalid immediately

How do I rotate signing keys?

```
# 1. Generate new key
openssl genpkey -algorithm ed25519 -out new-signing.key

# 2. Update the secret
kubectl create secret generic atb-agentauth-signing-key \
  --from-file=ed25519_privkey_pem=new-signing.key \
  -n atb --dry-run=client -o yaml | kubectl apply -f -

# 3. Restart AgentAuth
kubectl rollout restart deployment atb-agentauth -n atb
```

Old tokens will fail validation once the old key is removed.

Operations

How do I check if ATB is healthy?

```
# Broker health
curl -k https://localhost:8443/health

# AgentAuth health
curl -k https://localhost:8444/health

# OPA health
curl http://localhost:8181/health
```

How do I view audit logs?

Audit events are emitted to stdout in JSON format:

```
kubectl logs -n atb -l app=atb-broker -f | jq .
```

For production, configure a log aggregator (Splunk, ELK, Datadog).

What metrics are available?

ATB exports Prometheus metrics on `/metrics`:

Metric	Description
`atb_requests_total`	Total requests by status
`atb_request_duration_seconds`	Request latency histogram
`atb_poa_validations_total`	PoA validation results
`atb_approvals_total`	Approval requests

See Observability Guide for dashboards and alerts.

How do I debug policy decisions?

Enable OPA decision logging:

```
opa:
  env:
    OPA_DECISION_LOG: "console"
```

Or query OPA directly:

```
curl -X POST http://localhost:8181/v1/data/atb/poa/decision \
  -H "Content-Type: application/json" \
  -d '{"input": {...}}'
```

Integration

How do I integrate with my agent framework?

See the SDK documentation for Python and Go libraries.

Basic pattern:

```
# 1. Get PoA token
poa = atb_client.authorize(action="crm.contact.update", ...)

# 2. Make request with PoA
response = requests.get(
    "https://atb-broker/crm/contacts",
    headers={"X-Poa-Token": poa.token}
)
```

Can I use ATB with serverless functions?

Yes. The agent running in Lambda/Cloud Functions can: 1. Request PoA tokens via HTTPS 2. Include tokens in requests to ATB

You'll need to configure SPIFFE identity for serverless (e.g., using cloud provider attestation).

How do I add a new backend system?

1. Add a connector configuration:

```
{
  "connectors": [{
    "id": "my-system",
    "upstream_url": "https://my-system.internal",
    "path_prefix": "/my-system",
    "egress_allowlist": ["my-system.internal"]
  }]
}
```

2. Define actions in OPA policy:

```
low_risk_actions["my-system.status.read"]
medium_risk_actions["my-system.data.update"]
high_risk_actions["my-system.config.delete"]
```

3. Restart the broker

Troubleshooting

Request denied with "missing_poa"

The request requires authorization but no PoA token was provided.

Solution: Obtain a PoA token from AgentAuth and include it in the `X-Poa-Token` header.

Request denied with "invalid_poa_signature"

The PoA token signature doesn't match.

Causes: - Token was modified - Wrong signing key - Token from different AgentAuth instance

Solution: Request a fresh token from the correct AgentAuth.

Request denied with "token_expired"

The PoA token's `exp` claim is in the past.

Solution: Request a new token. Tokens are intentionally short-lived (5 min default).

Request denied with "insufficient_approvals"

High-risk action requires more approvers.

Solution: Collect additional approvals before the challenge expires.

AgentAuth returns "challenge_not_found"

The challenge ID doesn't exist or has expired.

Solution: Create a new challenge. Challenges expire after 5 minutes.

Compliance

Does ATB help with GDPR?

Yes. ATB supports GDPR through: - **Legal basis tracking**: Every action documents why it's permitted - **Accountable party**: Identifies who authorized the action - **Audit trail**: Complete record of all data access - **Constraints**: Limit data access to what's necessary

Does ATB help with SOX compliance?

Yes. ATB provides: - **Segregation of duties**: Dual control for sensitive actions - **Audit trail**: Immutable logs of all financial operations - **Access controls**: Action-specific authorization

Can I prove an agent was authorized to take an action?

Yes. Every PoA token is: - Cryptographically signed - Time-stamped - Linked to approver identities - Logged in the audit trail

Export the audit event and PoA token as proof.