Security and Authentication

- **academy.kspl.tech | Koenig AI Academy**

Prerequisites check

- **You need the structured logs from Chapter 5. If a tool call is not logged, you cannot audit sec**
- **academy.kspl.tech | Koenig AI Academy**

Authentication vs authorization

- Authentication answers "who is calling?" Authorization answers "may this caller do this action
- Authentication: request includes a bearer token that maps to user_123.
- Authorization: user_123 may read demo project files but may not list production secrets.
- Authentication: the MCP server receives FINANCE_API_KEY as an environment variable.
- academy.kspl.tech | Koenig AI Academy

Least privilege for connectors

- Least privilege means the connector receives only the access needed for its declared operations
- MCP makes it easy to expose capabilities. That ease is exactly why you must design them narrowl
- Avoid "admin token plus prompt rules" as a security model. Prompt rules are instructions; autho
- academy.kspl.tech | Koenig AI Academy

Authorization wrapper

- Put authorization before tool execution and before detailed logging of target data.
- roles: string[];
- function requirePermission(actor: Actor, permission: string) {
- if (!actor.roles.includes(permission)) {
- academy.kspl.tech | Koenig AI Academy

Human-in-the-loop approval

- **Some tools should not execute immediately even when authorized. Approval gates are appropriate**
- **A safe tool can return a pending action:**
- **"status": "awaiting_approval",**
- **"action": "send_invoice_reminder",**
- **academy.kspl.tech | Koenig AI Academy**

Try it next

- **Deploy a gateway with RBAC, rate limits, and JSONL auditing**
- **academy.kspl.tech | Koenig AI Academy**