**Title: Design Blueprint and Architecture for an AI Agent that Generates Model Context Protocols (MCPs)**

**🔧 PART 1: DESIGN BLUEPRINT**

**1. Objective**

To develop an AI agent that autonomously generates structured and domain-specific Model Context Protocols (MCPs) for users or downstream systems.

**2. Use Cases**

* Regulatory compliance (e.g., MAS TRM, GDPR, CBPR)
* Trade classification (e.g., HS Codes, dual-use goods)
* AI safety and governance contexts
* Cybersecurity SOP automation

**3. Features**

* Context extraction from documents, APIs, or prompts
* Role-based instruction generator
* Auto-formatting to MCP schema (JSON/YAML)
* Embedding references and external documents
* Constraint enforcement and validation

**4. Output Format**

{

"domain": "Trade Compliance",

"system\_prompt": "You are a customs classification assistant...",

"user\_guidance": "Classify goods based on description and HS schema.",

"input\_format": "{ \"product\_description\": \"\" }",

"output\_format": "{ \"hs\_code\": \"\", \"confidence\": 0.0 }",

"references": ["https://tradenet.gov.sg", "SGCO 2024"],

"constraints": ["Use Singapore classification", "No fallback to GPT guess"]

}

**5. Agent Capabilities**

| **Capability** | **Description** |
| --- | --- |
| Domain Inference | Determines which schema template to use |
| Prompt Engineering | Crafts system/user prompts with best practices |
| Data Linking | Extracts or fetches relevant datasets/document context |
| Validation & Scoring | Ensures MCP structure, relevance, and completeness |
| Output Packaging | JSON/YAML delivery, export to Notion, API or local |

**6. Agent Stack**

* **LLM**: DeepSeek, GPT-4o, Claude
* **Embedding DB**: FAISS, Chroma
* **Agent Framework**: LangGraph, AutoGen, CrewAI
* **Orchestration**: Python + FastAPI + Celery (if batch)
* **Optional GUI**: Next.js (admin) / Framer (frontend)

**📈 PART 2: HIGH-LEVEL ARCHITECTURE DIAGRAM**

**[System Components]**

+-----------------------------+

| User or Developer Input |

+-----------------------------+

|

v

+-----------------------------+

| Intent / Domain Detector | <--- NLP + classifier

+-----------------------------+

|

v

+-----------------------------+

| Document/Context Extractor| <--- PDF, DOC, API, RAG

+-----------------------------+

|

v

+-----------------------------+

| MCP Builder Agent | <--- Templates, PromptGen, Schema Builder

+-----------------------------+

|

v

+-----------------------------+

| Validation & Sanity Check |

+-----------------------------+

|

v

+-----------------------------+

| Output Delivery Layer | --> JSON/YAML, Notion, API, GUI

+-----------------------------+

Would you like a visual diagram export or implementation-ready code scaffold next?