

Enhancing Multi-Agent Collaboration

Context and AuthZ

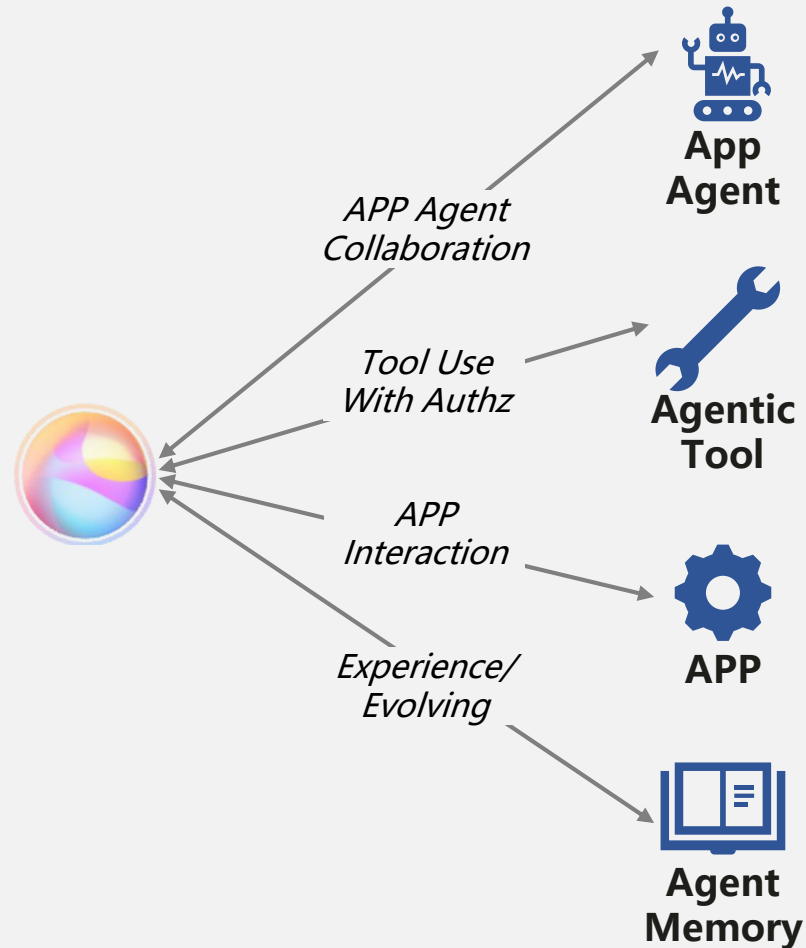
Jinyang Li, Yiyang Shao

lijinyang9@huawei.com; shaoyiyang@huawei.com

IETF 125 - HotRFC Lightning Talks

AI Agent Ecosystems on Terminals: Vision vs. Reality

Terminal Agent Ecosystem



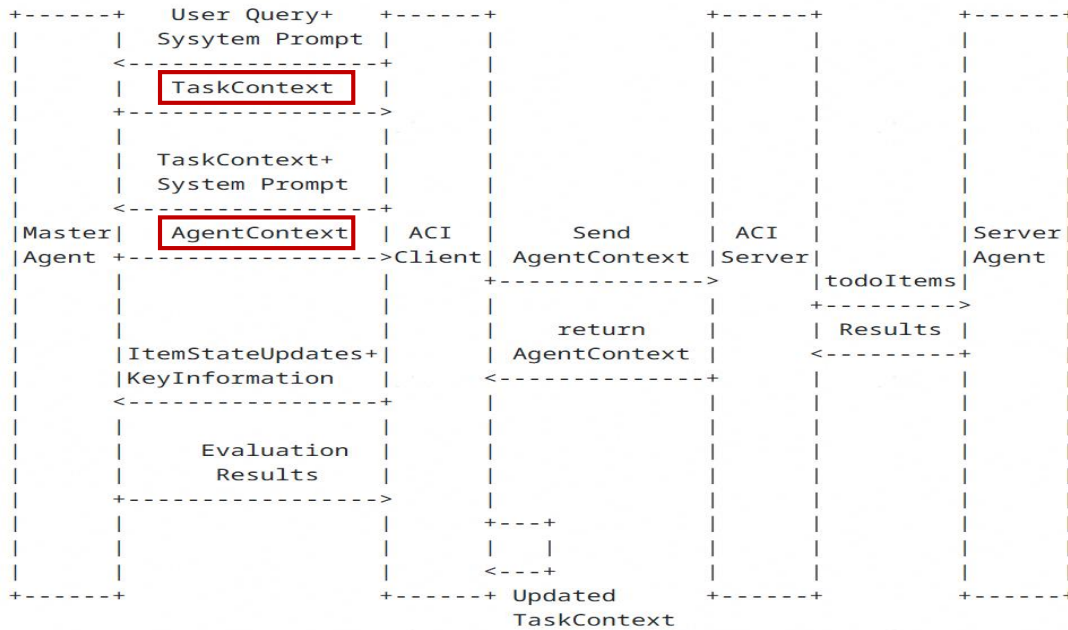
• Vision:

- **Scenario:** OS-level System Agents orchestrating multiple App Agents (e.g., travel planning, media processing).
- **User Value:** Frictionless, automated cross-app workflows directly on personal devices.

• Reality

- **Constraints:** Terminals face strict token, battery, and latency limits.
- **Challenges:** Current protocols (e.g., A2A, MCP) struggle with:
 - **Context Fragmentation:** Stateless, plain-text sync causes massive token overhead and execution failures.
 - **AuthZ Friction:** Reactive, step-by-step consent prompts lead to user fatigue and broken workflows.

Agent Context Enhancement for Multi-Agent Collaboration



```

"AgentContext": {
  "AgentID": "",
  "AgentName": "",
  "SubTaskID": "",
  "SubTaskName": "",
  "Dependencies": [],
  "Context/ContextURI": "",
  "todoItems": [ "itemId": "", "description": "" ],
  "ItemstateUpdates": [ "itemId": "", "state": 0 ],
  "KeyInformation": [ "itemId": "", "outputabstract": "" ],
}
    
```

*structured
semantic
schema*

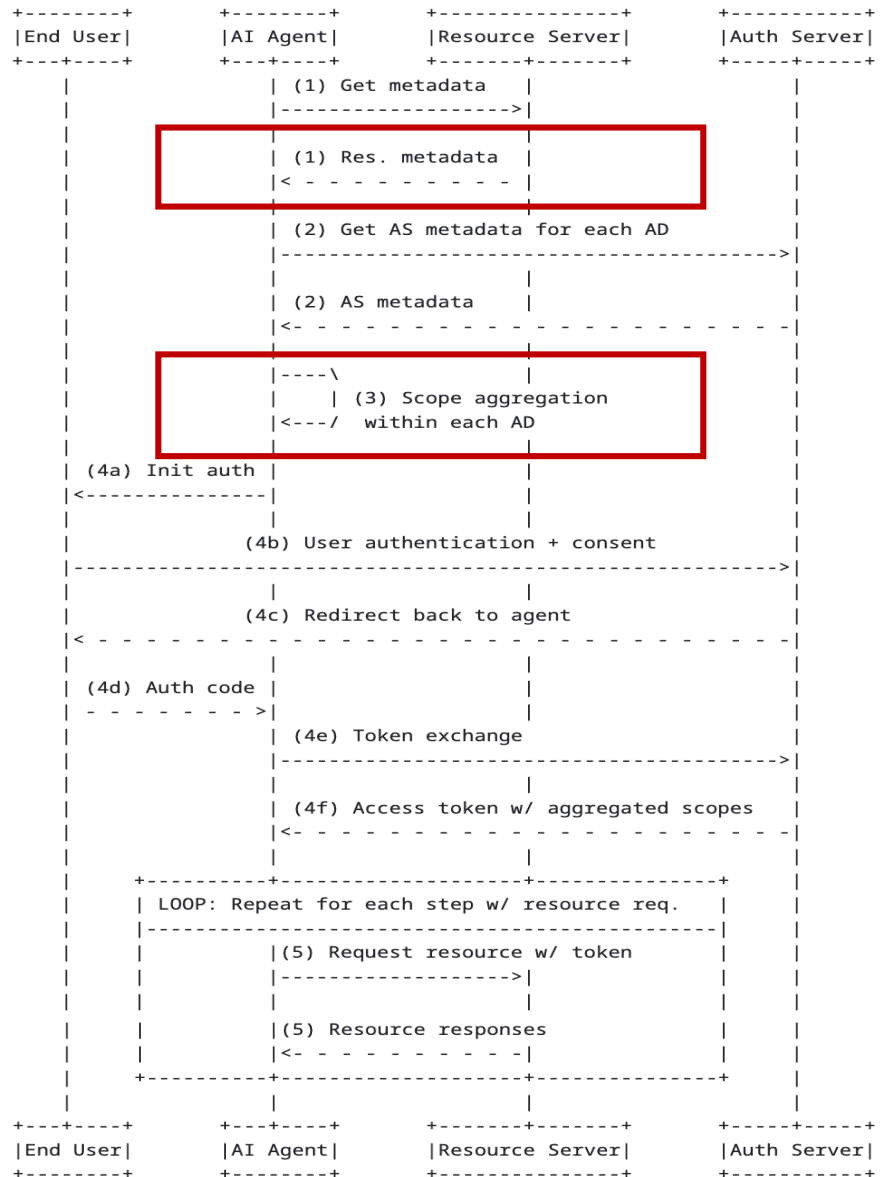
• Problem

- **Current State:** Agents rely on stateless, plain-text P2P exchanges without cross-agent task state management.
- **Example:** An OS System Agent coordinates a travel plan across Maps, Weather, and Booking App Agents.
- **Impact:** High token overhead, high latency, context loss

• Solution

- Transition from plain text to a structured semantic schema.
- Natively manage context boundaries, dependencies, and execution states
- **Draft:** [draft-chang-agent-context-interaction-01 - Agent Context Interaction Optimizations](#)

AuthZ Workflow Enhancement for Authorizing Tool



• Problem

- **Current State:** Existing agent protocols (e.g., MCP) handle OAuth 2.0 AuthZ flows in a reactive, challenge-triggered manner.
- **Example:** Agent executes a scheduling workflow across Email and Calendar, requesting authorization for multiple times
- **Impact:** Consent fatigue, mid-workflow failures, blocked automation

• Solution

- Record security requirements in resource metadata
- Aggregate required scopes to initiate ONE single authorization flow before execution.

```

{
  "name": "resource_identifier",
  "description": "...",
  "input_schema": { ... },
  "security": {
    "type": ["oauth2"],
    "scopes": ["scope_A"],
    "as_metadata": "https://server.example.com/.well-known/..."
  }
}
  
```

- **Draft:** [draft-jia-oauth-scope-aggregation-00 - OAuth 2.0 Scope Aggregation for Multi-Step AI Agent Workflows](#)

Summary

- **Challenges:** Terminal agents face strict constraints in tokens, latency, and user friction. Existing stateless and plain-text protocols cannot efficiently support complex workflows.
- **Our Proposals:** Shift towards structured, stateful, and pre-authorized AI protocols:
 - Structured Context Sync: draft-chang-agent-context-interaction-01
 - Aggregated AuthZ: draft-jia-oauth-scope-aggregation-00
- **Future Work:** Gather community feedback to optimize the proposals.

• Find more details in  openJiuwen



- **Let's Talk!** Catch me after this session for questions and discussions,
- or reach out via email: lijinyang9@huawei.com; shaoyiyang@huawei.com