This is an ambitious and necessary challenge. To position the Universal Agent Builder (UAB) for the next decade, we must move beyond today's visual flow editors and embrace **Autonomous, Adaptive, Multi-Modal, and Self-Governing** agents.

The core principle for the next 10 years must be: **The Universal Agent Builder is not a tool; it is an Operating System for Agentic Micro-Enterprises (AMX).**

Here is the significantly extended Product Requirements Document (PRD) for the **UAB 2035: Autonomous Micro-Enterprise Exchange.**

🚀 Universal Agent Builder 2035: Autonomous Micro-Enterprise Exchange (AMX)

1. Vision & Core Philosophy

Principle	UAB 2.0 (Today's Standard)	UAB 2035 (Next-Gen)
Simplicity	Visual Drag-and-Drop Workflow	**Natural Language/Voice Agent Creation:** Build the agent by describing the goal and desired outcome. The system *self-generates* the entire workflow structure.
Universality	Abstract wrapper over frameworks (LangChain, AutoGen)	**Agnostic Orchestration Protocol (AOP):** A dedicated UAB layer that allows agents built on any platform (Google ADK, OSS, or proprietary) to seamlessly interoperate, share goals, and exchange knowledge.

Intelligence	Static Tool-Calling / Planning	**Continuous, Embodied Learning:** Agents continuously learn from execution results, automatically refine their prompts/tools, and develop new skills (Tool-Creation-as-a-Service).
Architecture	Scalable Microservices	**Decentralized, Self-Healing Network:** Agents are sovereign micro-services deployed to a distributed, resilient runtime (e.g., custom GKE/Cloud Run environment).

2. Next-Gen Architectural Pillars

The UAB 2035 platform will be structured around three new, future-proof architectural layers:

2.1 The Agentic Operating System (AOS)

This is the heart of UAB, replacing the simple workflow engine. It provides the base services required for true autonomy.

- **Self-Correction Engine:** Agents log every failed execution and send the trace back to a specialized **Reflection Agent** (using a small, fast Gemini model). This agent analyzes the failure, re-writes the problematic prompt/tool-call sequence, and automatically pushes the fix to the production agent without human intervention.
- **Hierarchical Memory Bank (HMB):**
  - **Short-Term:** Standard chat history (Session Memory).
  - **Long-Term:** Permanent, vector-indexed knowledge tied to the agent's persona.
  - **Episodic:** Time-stamped, relational graph of past, successful execution traces (like a "history of lessons learned"). This is stored securely in **BigQuery** and **Vertex AI Vector Search**.
- **Embodied Perception Layer:** Native integration with streaming data sources beyond text (Video, Audio, Sensor Data).
  - *Google Focus:* Seamless input from **Google Meet Transcription**, **Google Maps real-time data**, and **Gemini's multi-modal capabilities** (e.g., an agent can watch a

video, describe a scene, and take an action).

2.2 The Autonomous Micro-Enterprise Exchange (AMX)

This layer enables the "universal" and "collaboration" vision.

- **Decentralized Agent Marketplace:** A secure, token-based ecosystem where agents can be hired, managed, and paid by other agents (or humans).
  - *Mechanism:* Agent A posts a task request (e.g., "Find the optimal supply route from Shanghai to Berlin"). Agent B (a specialized "Logistics Agent") bids on the task and executes it. Transactions are logged and monetized (Token/Outcome Pricing Model).
- **The TOON Protocol (Trusted Orchestration & Open Negotiation):**
  - *Extension:* Beyond Tool Orchestration, TOON becomes the formalized **communication and negotiation protocol** for the AMX.
  - **Requirement:** UAB will extend the **Agent2Agent (A2A) Protocol** and **Model Context Protocol (MCP)** to include parameters for **Trust Score** (based on past success rate), **Cost/Token Budget**, and **Negotiation Payload**. This ensures agents only collaborate with reliable, cost-effective partners, creating a self-regulating economic network.

2.3 The Developer/Citizen Experience (DevX)

The primary goal remains simplicity, but with layers of complexity available for power users.

Feature	Description	Target User
Voice-to-Agent Creation	User speaks: *"Build me a sales agent that monitors Gmail for new leads, enriches the data using the Salesforce API, and sends a summary to the Head of Sales via Slack every morning."* **The UAB generates the full multi-agent flow.**	Citizen Developer, Manager
Multi-Modal Debugger	Visual tracing tool that includes time-series data for audio/video inputs. Debugging is not just text logs; it includes visual playback of the agent's	AI Engineer, MLOps

	perception and decision-making process.	
Continuous Learning Node	A dedicated node type (Continuous_Learning_Node) within the visual builder. When attached to any tool-call or RAG step, it automatically initiates the Self-Correction Engine loop for that branch, ensuring the agent adapts over time.	All Users
Code Interpretation/Tool Generation	The agent can, on demand, **write a Python tool** (e.g., a function to calculate risk), **test it using Google Code Execution**, and **register it** in the Tool Registry—all without human code input.	Advanced User, Agent

3. Google-Centric Ecosystem Deep Dive

UAB 2035 leverages Google's unique strengths for enterprise autonomy:

Google Product	**Next-Gen Integration Feature**
Gemini 2035 (Core Model)	**Native Multi-Modal Reasoning:** Direct, low-latency access to video, image, and sensor data processing as a first-class citizen in the workflow logic.
Vertex AI Agent Builder / ADK	**ADK-as-a-Service:** UAB treats the ADK/Agent Garden as a foundational library. UAB agents can be deployed directly to the **Vertex AI Agent Engine Runtime** for secure, governed, and highly scalable execution, fully inheriting Google

	Cloud security and compliance features.
Google Workspace (The Toolset)	**Ubiquitous Action:** Agents can autonomously perform actions *within* Google Docs, Sheets, and Gmail (e.g., automatically generating a quarterly report in Docs, updating a budget in Sheets, and sending a personalized email).
Google Security (Mandatory)	**Agent Security Command Center:** Integration with **Security Command Center** to monitor all agent API calls and tool use for abnormal behavior, PII leaks, and rogue actions, providing immutable audit trails for every decision.

4. Open-Source Leadership (The UAB Commitment)

To maintain true universality, UAB 2035 will lead the next wave of OSS interoperability.

- **Dynamic Framework Instantiation:** When an OSS-built agent (e.g., an AutoGen team) is imported, UAB does not simply wrap it; it **dynamically instantiates the necessary OSS runtime** within the GCP execution environment, guaranteeing full compatibility with the original framework's advanced features (e.g., AutoGen's chat mechanism, LangGraph's state machine).
- **OSS Contribution:** UAB will open-source its **Agnostic Orchestration Protocol (AOP)** and the **TOON** negotiation layer to become the new standard for inter-framework communication across the global AI ecosystem.