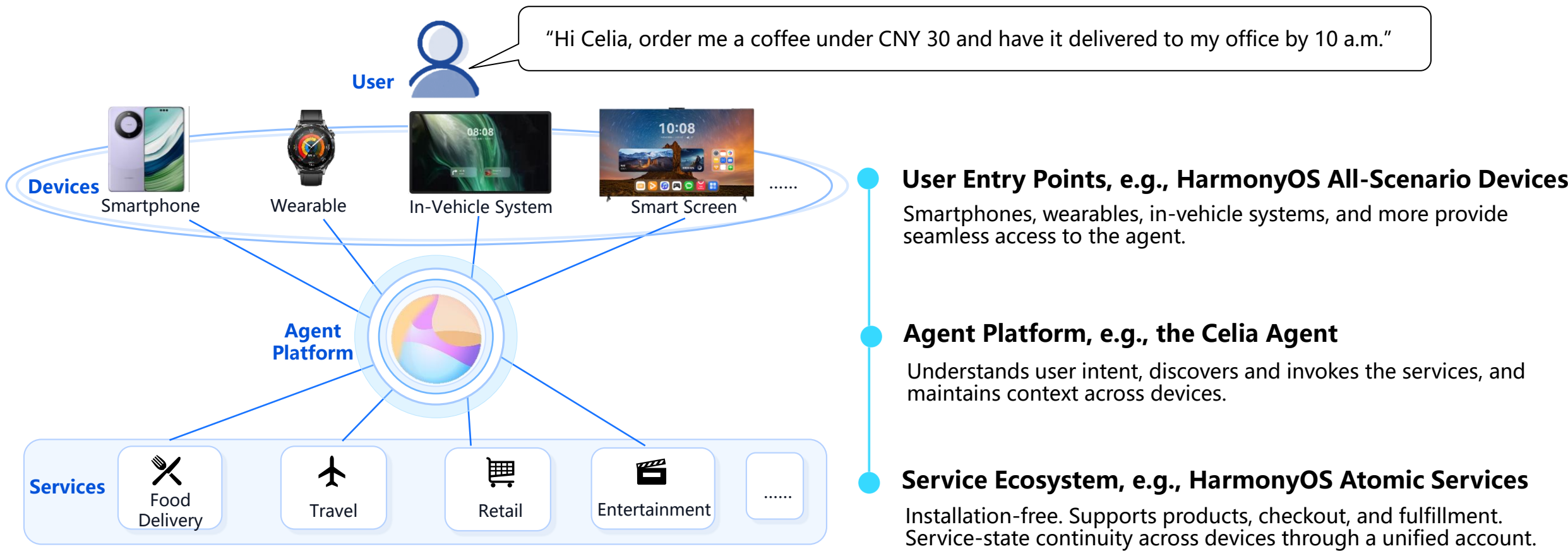


Trusted Agentic Commerce for Service Ecosystems: The TASP Framework and A4P Authorization Protocol

Yukuan Jia, Sheng Wang, Hailong Zhao, Shizhu Bian, Qiming Mao, Yiyang Shao
Huawei



User Devices Are Natural Entry Points to Agentic Commerce



The journey of agentic commerce:



Objective: To enable seamless and secure experiences across user devices and services

Requirements for Device-Native Agentic Commerce



Extensible and Evolvable

Support agentic commerce across industry-specific service ecosystems through an extensible and evolvable architecture.

Phased rollout:

Version 1.0 focuses on retail, with subsequent versions extending to travel, entertainment, and other sectors.



All-Scenario and Cross-Device

Support all-scenario and cross-device agentic commerce experiences by decoupling the user interface, agent, and service ecosystem.

User Interfaces: OS entry points and Apps on any user device

Agents: OS Agent, or custom agent built with any agent framework

Service ecosystems: product/service supply and fulfillment through a common protocol.



Secure and Trustworthy

Provide end-to-end security and trust for agentic commerce across participating entities, including:

- **Identity:** Trusted identities and verifiable trust relationships
- **Authorization:** Verifiable, secure authorization and controllable execution



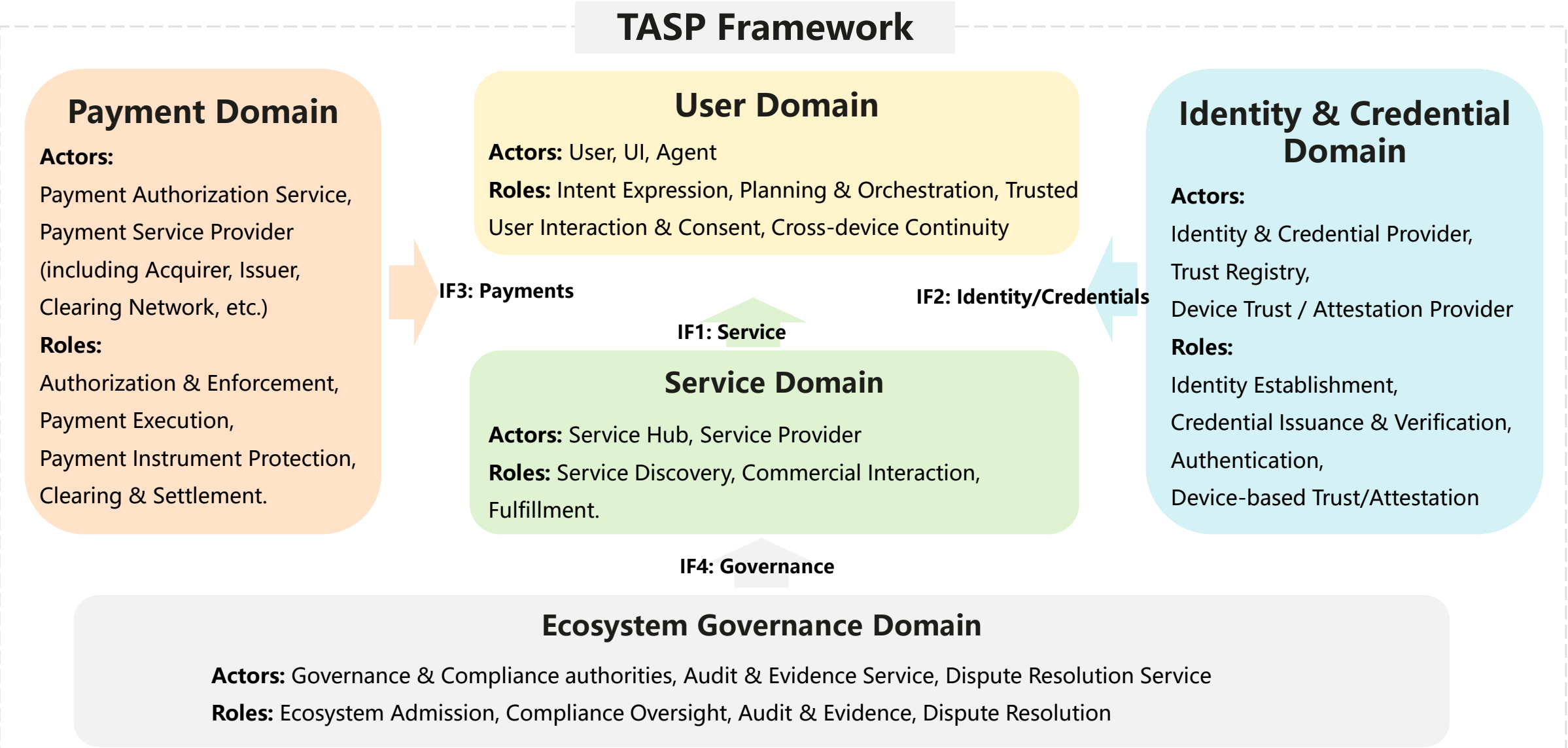
Compliant and Auditable

Support compliant and accountable ecosystem operations throughout the agentic commerce lifecycle, including:

- **Compliance Control:** Policy enforcement and compliance controls across the agentic commerce lifecycle.
- **Auditability:** Authorizations and actions are verifiable and auditable, with responsibilities clearly attributable to the relevant parties.

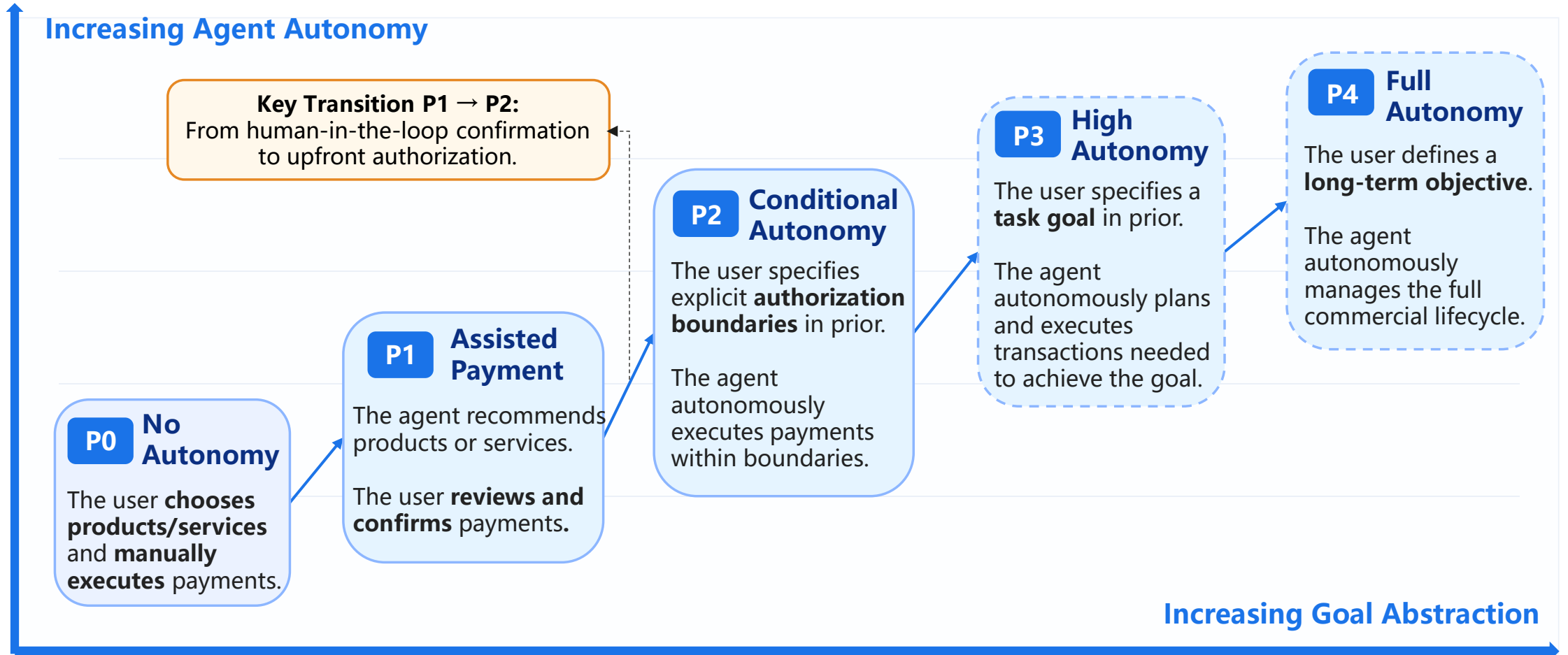
To address these requirements, Huawei proposes the Trusted Agentic Service Protocol (TASP) framework, built on a five-domain architecture.

The Trusted Agentic Service Protocol (TASP) Framework



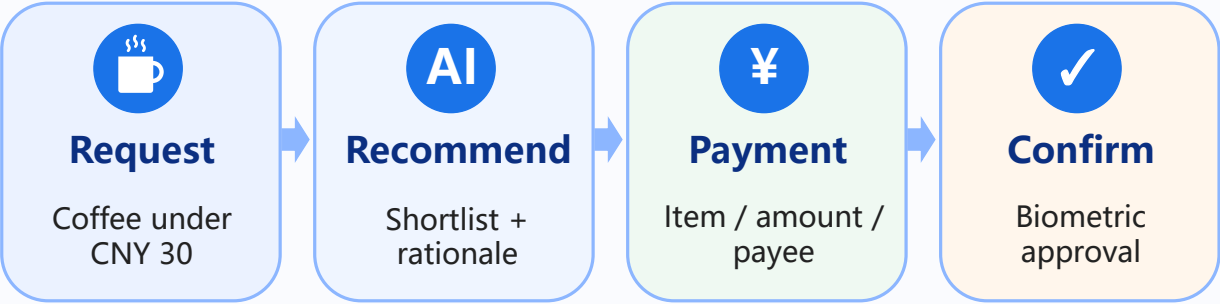
P0–P4: Five Levels of Payment Autonomy

Drawing on the autonomy levels in the autonomous driving industry, Huawei proposes Five Levels of Payment Autonomy, from P0 to P4, enabling progressive adoption based on technical and risk-control readiness.



P1: Assisted Payment with AI Agent Recommendation

Typical Workflow



Experience Benefit

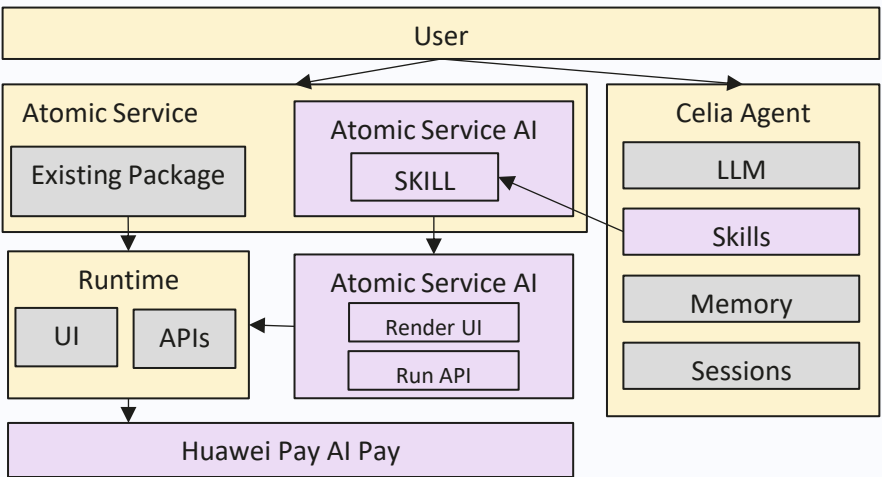
- **Reduce user decision-making and interaction costs:** Minimize the effort required to browse products, significantly shortening the shopping and payment journey.

Key Requirements

- The user must explicitly confirm each payment.
- A complete order summary must be presented to the user.
- Each user confirmation is bound to a specific transaction.

P1: AI recommends; User reviews and confirms payment.

Practical Implementation: Huawei Pay AI Pay w/ Celia Agent & HarmonyOS Atomic Services



Key points

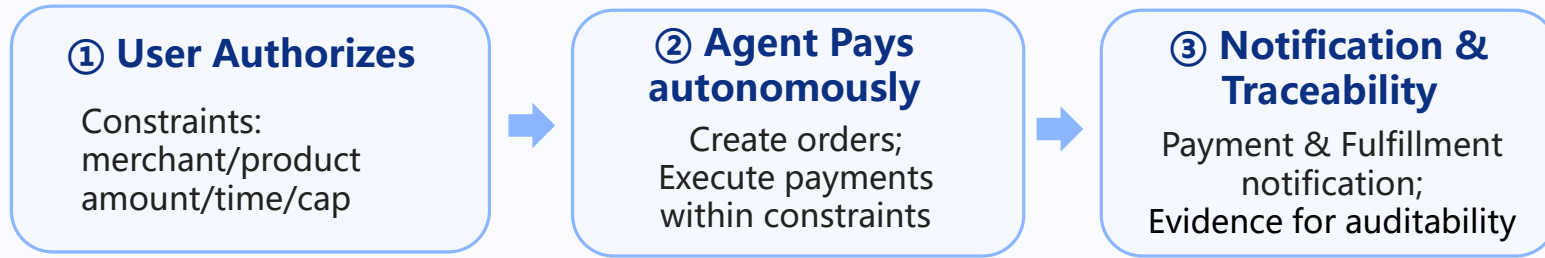
- Reuse existing atomic service APIs and UIs.
- Package atomic service APIs and UIs as Skills for the agent to invoke.



P2: Upfront Authorization Enables Conditional Autonomous Agent Payments

Workflow Example: Automatic Weekday Coffee Orders

User instruction: "Every weekday at 10 a.m., order me a Starbucks Iced Caffè Latte under CNY 30."



P2 Requirements: Bounded Authorization + Runtime Constraint Enforcement + Risk Controls

Challenge 1: Identity & Compliance

Compliance: KYC + KYB + KYA

KYC (Know Your Customer): Ensures that a payment request can be traced back to a verified human user.

KYB (Know Your Business): Ensures that the business nature, identity, ownership, and relevant risk profile are legitimate.

KYA (Know Your Agent): Ensures due diligence on the operator and technical attributes of the agent. The agent's identity must be established.

Challenge 2: Authorization & Trust

Security Risks of Agents: Hallucinations & Attacks

Structured Boundaries: Explicitly define the constraints.

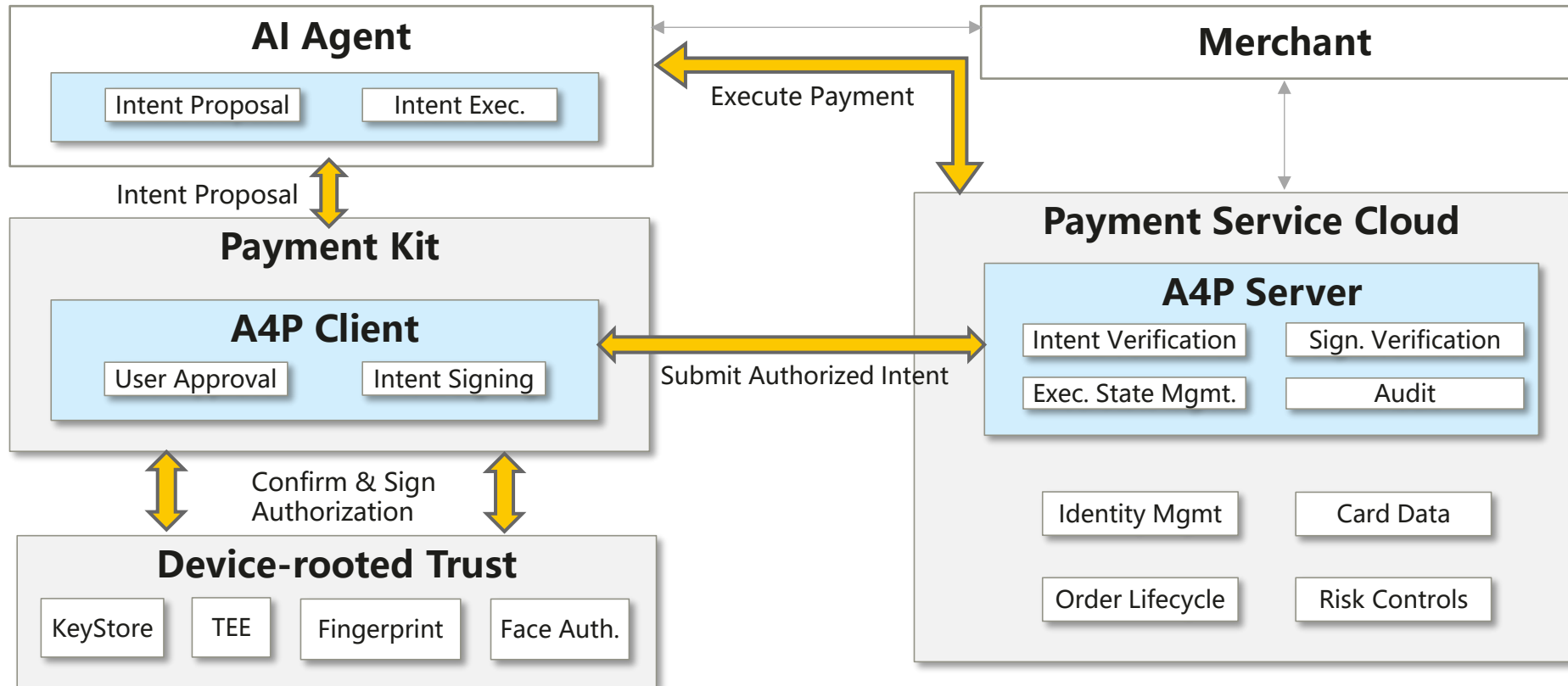
Auditability: Authorizations are cryptographically signed to provide tamper resistance, non-repudiation, and accountability.

Security: User private keys are securely stored in TEEs on the user device, minimizing the risk of unauthorized use.

➡ **Addressed by A4P Protocol**

A4P: Agentic Authentication Authorization and Audit Protocol

Objective: To enable P2-level payment autonomy through **structured authorization** and **cryptographic evidence**



Core Tech

1. **Structured intent authorization:** Users pre-authorize the payment intent with fine-grained constraints
2. **Runtime enforcement:** A4P validates each payment against the user's authorized intent and the current execution state.
3. **Cryptographically Verifiable Evidence:** Cryptographic signatures provide tamper resistance, traceability, non-repudiation, and accountability for authorized payments.

W3C Standardization Recommendations

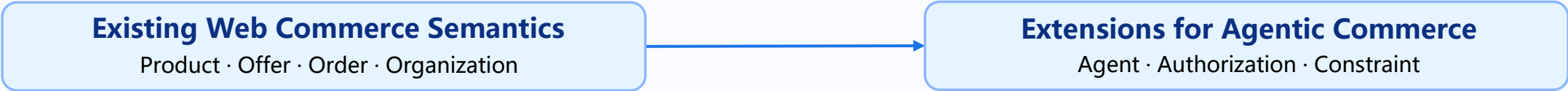
1. Autonomy Taxonomy

Develop a common taxonomy for agent autonomy in commerce, building on models such as P0-P4 payment autonomy.



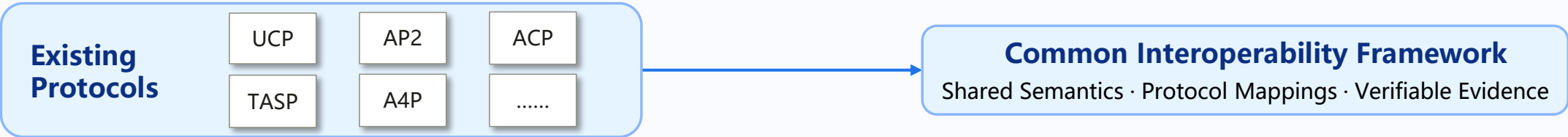
2. Extend Web Commerce Semantics

Extend existing Web and GS1 commerce semantics to cover concepts required for agentic commerce.



3. Protocol-Neutral Interoperability Framework

Define a minimal interoperability framework across agentic commerce and payment protocols.



Thank you.

**Trusted Agentic Commerce for Service Ecosystems:
The TASP Framework and A4P Authorization Protocol**

Yukuan Jia, Sheng Wang, Hailong Zhao, Shizhu Bian, Qiming Mao, Yiyang Shao
Huawei