AGENTIC COMMERCE

How Commerce Survives 2030

STRATEGY BOOK

Agents are revolutionizing commerce. This strategy book analyzes the mechanics of this disruption and provides you, as a merchant, platform operator, tech decision-maker, or investor, with concrete strategies for the era of Agentic Commerce.

AUTHOR

Stefan Hamann

VERSION

v1.3 – January 2026

Contents

Introduction

Definition: Agentic Commerce

Agents buy on behalf of humans. They make purchasing decisions, execute transactions, and manage after-sales—with the user's permission, within defined rules and budgets.

What "autonomous" really means:

Not "independent without control," but "delegated with limits and an audit trail."

Two Modes:

- **Agent-assisted:** Agent recommends, human decides
- **Agent-executed:** Agent decides and acts within policies

The transition between these two modes is fluid—and that is precisely where the strategic opportunity lies.

Terminology in this Strategy Book:

This document uses stable terms and defines them in the glossary.

- **Agent** – AI system that acts on behalf of humans
- **Trust Score** – Internal KPI construct that bundles observable signals
- **Protocol-capable** – Graded integration: Findable (UCP/Feed), Buyable (AP2/ACP), Trust-ready (TAP), Experience-ready (AXP)
- **Emotional Value Zone** – Area with non-automatable added value

Thesis: Key Thesis

Market power is no longer created through visibility, but through machine-readability.

This is the central insight. Everything else follows from it.

The Three New Currencies:

1. **Protocol-capable** – Whoever is reachable via UCP, AXP, and AP2 will be found
2. **Trust Score** – Whoever provides verified quality signals will be preferred
3. **Emotional Value Zones** – Whoever offers non-automatable experiences differentiates themselves

Every section of this strategy book is measured against this thesis. The question is always: *How does this affect my position with protocols, trust, or experience?*

Prolog: The Last Merchant

A fictional morning walk through a shopping street in the year 2030: almost all shops have disappeared. Purchases are handled invisibly in the background by agents. Only one shop is open—"The Last Merchant."

This opening scene outlines the guiding question of this strategy book: **What remains when agents take over a large part of the customer journey?**

This strategy book argues that commerce will fundamentally transform—but not disappear. The winners will be those who understand: (1) which parts of the value chain fall to agents, (2) which parts can be defended through human strengths, (3) what the new architecture of protocols and trust looks like, and (4) what the operating model of an agent-capable merchant entails.

Target Groups

Merchants: Playbook for transformation—data strategy, trust signals, operating model.

Tech Decision-Makers: Architectural decisions, in-house development vs. partners, protocol landscape.

Investors: Value shift in architecture, moats, winner-loser hypotheses.

Methodology and Sources

The analyses are based on publicly available announcements, protocol specifications, and scenario analyses. Where specific numbers are mentioned, they are to be understood as *scenarios*, not as deterministic forecasts. Primary sources are linked in the text.

The Agentic Commerce Mental Model

This diagram is the one graphic that explains everything. It is referenced in every part and forms the basis for all strategic decisions.

The Experience Layer serves three target groups:

- **Agent Experience:** Machine-readable signals via AXP (quality signals, structured product data, trust indicators). Agents *read* experience as a basis for decision-making.
- **Human Experience:** Immersive interfaces (3D, AR, configurators, video consulting). Humans *experience* commerce emotionally and sensorially.
- **Hybrid Experience:** Agent-assisted scenarios where agents pre-filter and humans make the final decision. Both modalities work together.

Implication: Experience is not a marketing feature, but a structural lever in the Agent Funnel. Those who build experience only for humans will lose agent traffic. Those who build experience only for agents will lose margin.

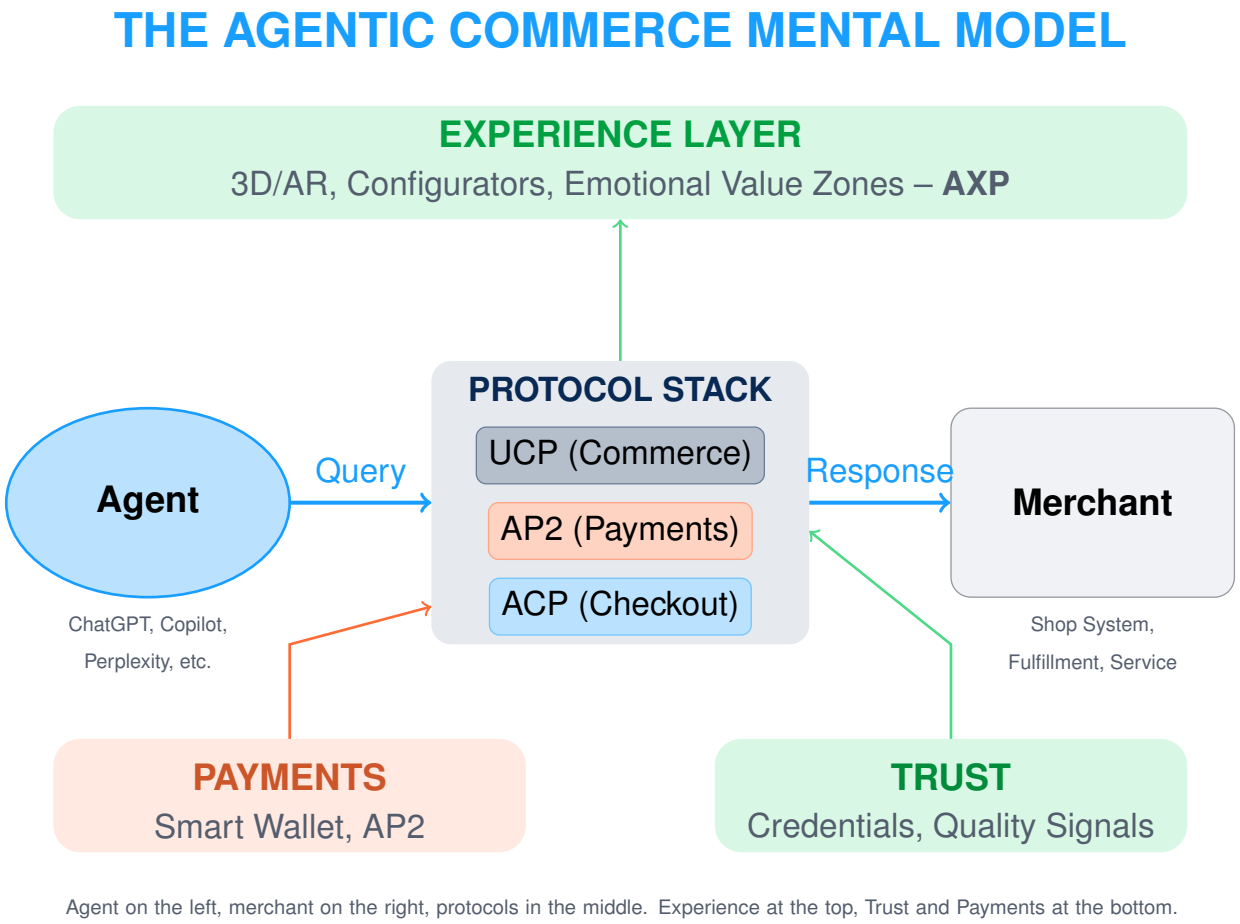

Figure 1: The Agentic Commerce Mental Model: Agent (left) communicates with the merchant (right) via the protocol stack (middle). Experience Layer (top) differentiates, Trust and Payments (bottom) secure the process. **Reference for all parts.**

Resources and Ecosystem

Agentic Commerce Developer Hub (https://agentic-commerce.dev):

The portal for AXP (Agentic Experience Protocol) and Alliance content. Offers:

- AXP documentation and reference implementations
- Playground for testing experience flows
- Strategic whitepapers and research

Other Protocol Portals:

- **ACP (OpenAI/Stripe):** https://agenticcommerce.dev
- **UCP (Google):** https://developers.google.com/merchant/ucp

Agentic Commerce Alliance (https://www.agentic-commerce.org):

The global industry alliance for open standards in Agentic Commerce. Founded in July 2025 by Shopware under the leadership of Stefan Hamann. The Alliance brings together merchants, technology providers, payment providers, and AI companies with the goal of developing open protocols and preventing monopoly structures.

- **Mission:** Human Value Preservation in an automated world

- **Focus:** Open standards, interoperability, merchant sovereignty
- **Members:** Leading retailers, payment providers, tech companies

Expert Blog and Research (https://www.agentic-commerce.sh):

Stefan Hamann's personal platform with strategic analyses, deep dives, and current developments in Agentic Commerce:

- **Whitepapers:** Technical and strategic guides
- **Protocol Updates:** Latest developments in UCP, AXP, AP2
- **Industry Reports:** Analyses of McKinsey, Morgan Stanley, IBM/NRF

Commerce Protocols (Details in Part III):

- **UCP:** Universal Commerce Protocol – End-to-end orchestration
- **AXP:** Agentic Experience Protocol – Rich content & quality signals
- **AP2:** Agent Payments Protocol – Secure payment mandates
- **A2A:** Agent2Agent Protocol – Multi-agent coordination
- **ACP:** Agentic Commerce Protocol – Instant checkout (OpenAI/Stripe)
- **StoreSync:** PayPal's catalog and cart orchestration

PART I

Strategic Context

1 The Age of Agents

If you skip this chapter: You continue to optimize for SEO and ads while agents are already buying via protocols. This is not a minor mistake—it's strategic blindness.

1.1 The Mechanics of Disruption

1.1.1 Why Distribution is Tipping

The fundamental disruption lies in the **shift of the gatekeeper position**. Until now, three actors controlled access to the customer:

Current Distribution: A significant portion of e-commerce traffic starts in search engines (Scenario: 30–50%, varies by category and region), marketplaces, and social platforms. These gatekeepers aggregate findability and redirect traffic.

Why Agents Change This: Agents know the need before the user explicitly searches. They compare across platform boundaries and curate based on persistent user preferences. Agents organize findability differently: not through central portals, but through direct protocol requests to merchant APIs.

Consequence: Gatekeepers are transforming from traffic aggregators to protocol, wallet, or trust layers. Merchants with direct protocol connectivity win—regardless of their previous SEO position or marketplace presence.

Key Terms (detailed in the glossary):

- **Protocol-capable** – Graded: *Findable* (UCP or Feed + StoreSync), *Buyable* (AP2 or ACP), *Trust-ready* (TAP or comparable credentials), *Experience-ready* (AXP or similar experience signals)
- **Trust Score** – Internal KPI construct from quality signals. External agents use similar signals but with their own weighting
- **Agent Order** – Order initiated by an agent using a verified agent identity
- **Emotional Value Zone** – Area with non-automatable added value (sensory experience, identity, community)

1.1.2 The New Funnel – with Merchant Levers

Glossary of Metrics:

- **API Reach:** The percentage of agents that can technically reach your assortment (feeds plus

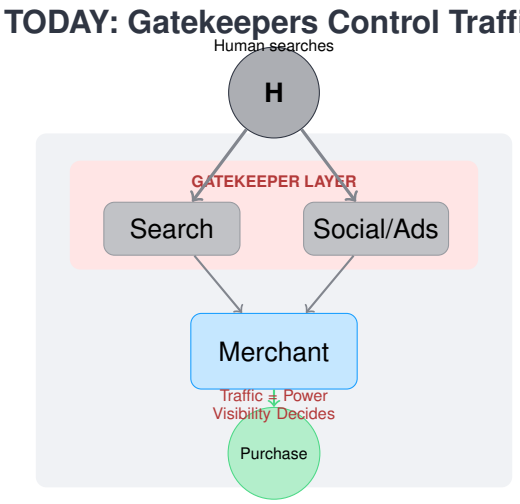

Figure 2: Today: Gatekeepers (search, social, ads) control access to the customer. Merchants pay for visibility.

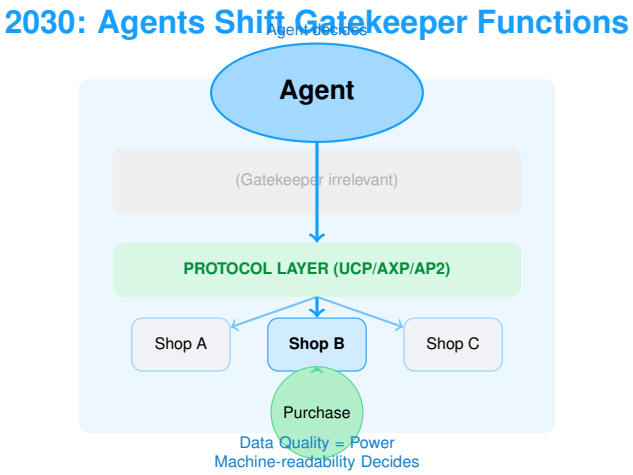

Figure 3: 2030 Scenario: Agents bypass gatekeepers through direct protocol coupling. Best data wins, not best ads.

Phase	Classic → Agent	Your Lever	Metric
Awareness	Ads → Protocol Findability	**UCP Compliance**	API Reach
Interest	Website → Preference Matrix	Quality Signals	Trust Score
Desire	Product Page → AXP Data	**Experience Content**	Embedding Rate
Action	Checkout → API Transaction	Response Time	Latency P95
Loyalty	Newsletter → Preference Learning	Return Excellence	NPS

Table 1: Funnel Transformation: This table shows how each phase changes—so you can prioritize the right levers.

APIs plus availability).

- **Trust Score:** Internal KPI construct based on verification, returns, and incident history. External agents use similar signals with their own weighting.
- **Embedding Rate:** The percentage of sessions in which your experience component is actually rendered.
- **Latency P95:** 95th percentile of response time for agent requests. Critical, as agents have hard timeouts.

What you can derive from this:

- **API Reach below 80%?** Then more than 20% of agents cannot find your assortment—you are simply invisible to a large portion of agent traffic.
- **Trust Score beats Conversion Rate:** Agents do not evaluate you based on classic conversion metrics, but on your Trust Score. A low score leads to lower prioritization.
- **Latency P95 is conversion-critical:** Agents have hard timeouts (typically a few seconds). APIs that are too slow lead to cancellations—latency is not just a tech detail, but a direct revenue factor.

1.1.3 Value Flows in the New Model

Three flows in Agentic Commerce: Data, trust, and money flow through different channels. The following three diagrams show each flow separately—with identical actors in the same positions for easy comparison.

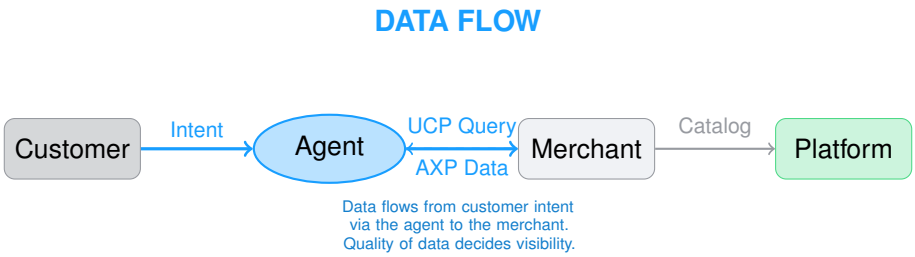

Figure 4: Data Flow: Intent → Agent → UCP Query → Merchant. Back channel: AXP product data.

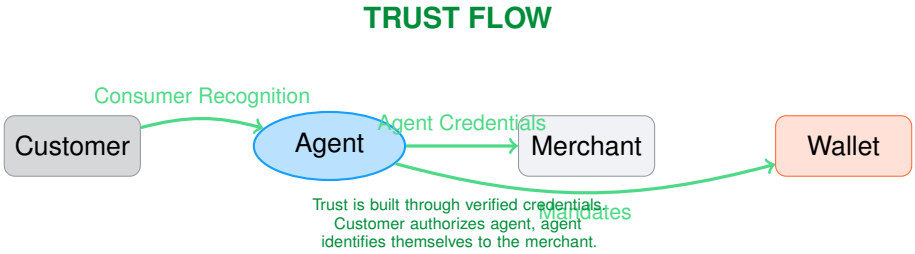

Figure 5: Trust Flow: Consumer Recognition → Agent Credentials → Merchant. Mandates to Wallet.

Risk: Transformation of Gatekeepers

The following actors must transform their roles or lose their gatekeeper positions: SEO/SEA agencies, affiliate networks, price comparison portals, classic review platforms, retargeting

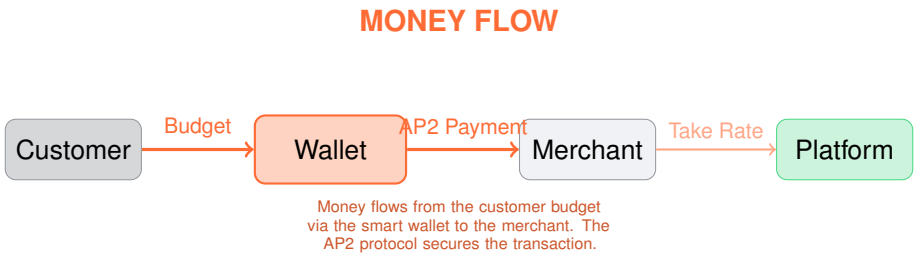

Figure 6: Money Flow: Budget → Smart Wallet → AP2 Payment → Merchant. Take rate to platform.

providers. Successful ones will transform into protocol, wallet, or trust layers.

1.2 Evidence: Milestones 2024–2026

The following timeline documents the technical breakthroughs and market milestones that have turned Agentic Commerce from a vision into an operational reality.

Time	Development and Primary Source	Status
Nov 25, 2024	**Anthropic MCP:** Standardizes LLM data access and tool integration.[1]	Productive
Jan 23, 2025	**OpenAI Operator:** First agent for browser control and purchases.[2]	Pilot
Sep 16, 2025	**Google AP2:** Agent Payments Protocol with mandates and verifiable credentials.[3]	Initial Release
Sep 29, 2025	**OpenAI Instant Checkout + ACP:** ChatGPT gets checkout based on ACP.[4]	Productive
Oct 14, 2025	**Visa TAP:** Trusted Agent Protocol for agent identity and fraud prevention.[5]	Available
Oct 28, 2025	**PayPal Agentic Commerce:** Launch of Agentic Commerce Services.[6]	Rollout
Nov 25, 2025	**PayPal + Perplexity:** Instant Buy integration with StoreSync.[7]	Rollout
Jan 8, 2026	**Microsoft Brand Agents:** Copilot checkout, referencing ACP as standard.[8]	Productive
Jan 11, 2026	**Google UCP 1.0:** Universal Commerce Protocol, endorsed by 20+ partners.[9]	Initial Release

Table 2: Timeline: The path to Agentic Commerce (2024–2026). **Productive** = Live in market, **Initial Release** = Published specification, **Pilot** = Test phase.

Definition: MCP as Integration Layer

The Model Context Protocol (MCP), announced by Anthropic on November 25, 2024, is the common integration layer supported by multiple agent platforms (Anthropic, OpenAI, Google). **Before MCP**, you had to build a custom API for every AI bot. **With MCP**, you expose a standardized "resource server" that Claude, ChatGPT, Gemini, and other LLMs can read equally. UCP, ACP, and AP2 support MCP or are compatible with it—they build on it but are independent commerce protocols.

Hypothetical Scenario: Perplexity Shopping Integration

The Perplexity shopping integration developed in three stages:

- **July 2025:** Comet Browser first availability (Early Access)
- **October 2025:** Broader launch with shopping feature
- **Nov 25, 2025:** PayPal Instant Buy integration announced

The agent takes over product selection, merchant comparison, and checkout. *Status: Rollout phase, no publicly communicated volumes.*

1.3 Market Potential: The Numbers Behind the Hype

The strategic relevance of Agentic Commerce is supported by independent analyses from leading consulting firms and financial institutions:

Category	Source	Forecast	Status
Spending Shift	Morgan Stanley[10]	**$190–385 billion** US e-commerce spending by agentic buyers by 2030	Scenario*
Orchestrated Revenue	McKinsey[11]	"Seismic shift" – agents execute multi-step commerce flows	Analysis
Survey Insights	IBM + NRF[12]	Fundamental change in consumer spending expected	Survey
Tech Readiness	Google Cloud	Retail readiness as a critical competitive factor	Productive

Table 3: Market forecasts by category: *Spending Shift* = Revenue shift, *Orchestrated Revenue* = Agent-controlled flows, *Survey Insights* = Consumer survey, *Tech Readiness* = Infrastructure. *Scenario values are estimates, not forecasts.

Strategic Implication (McKinsey): Agentic Commerce is "not just a trend, but a structural leap." Traditional e-commerce optimizes for clicks, conversions, and creative campaigns. Agentic Commerce shifts *decision rights* from humans to intelligent autonomous agents.

Thesis: Disruption of Distribution

The actual disruption is the loss of the gatekeeper position. Merchants with direct protocol connectivity win—regardless of their previous SEO position.

Actionable Recommendation: What you do differently now

This week:

- Analyze budget split: SEO/SEA vs. data quality/API readiness
- **First artifact:** One page with current split and target split

Next 14 days:

- Introduce KPIs "Agent Orders" and "API Reach" in the dashboard
- **Responsibility:** Head of E-Commerce or CTO

Next 30 days:

- Appoint an Agent Channel Lead (not IT, not marketing alone)

2 Customer Journey 2030

If you skip this chapter: You continue to optimize for website visits and product page views while the real conversion has long since been decided in API responses and Trust Scores.

The customer journey changes fundamentally when agents act as intermediaries. Classic funnels (AIDA: Awareness, Interest, Desire, Action) remain as a concept—but the *actors* and *touchpoints* shift. Instead of humans visiting websites, agents interact with APIs. Instead of emotional advertising messages, structured data and Trust Scores decide.

This chapter shows you phase by phase which risks arise and how to counter them. The table summarizes the most important error patterns and assigns the appropriate countermeasure and relevant protocol to each.

2.1 Phase-by-Phase with Countermeasures

Phase	Risk (Error Pattern)	Your Countermeasure	Protocol
Need	False Positives	Confidence Thresholds	MCP
Research	Incomplete Data	**Schema Validation**	UCP
Selection	Hallucination	**Structured Data only**	AXP
Checkout	Payment Reject	Retry + Fallback	ACP/AP2
After-Sales	Sync Error	Event Sourcing	Webhooks

Table 4: Journey phases with risks: This table shows what can go wrong and how you prevent it.

What you can derive from this:

- Hallucination is not an LLM problem—it is a data quality problem. Your countermeasure: Structured Data.
- Payment Reject is the most expensive mistake. Retry + Fallback must be automated.
- After-sales sync errors destroy the Trust Score. Event sourcing is not an option, but a requirement.

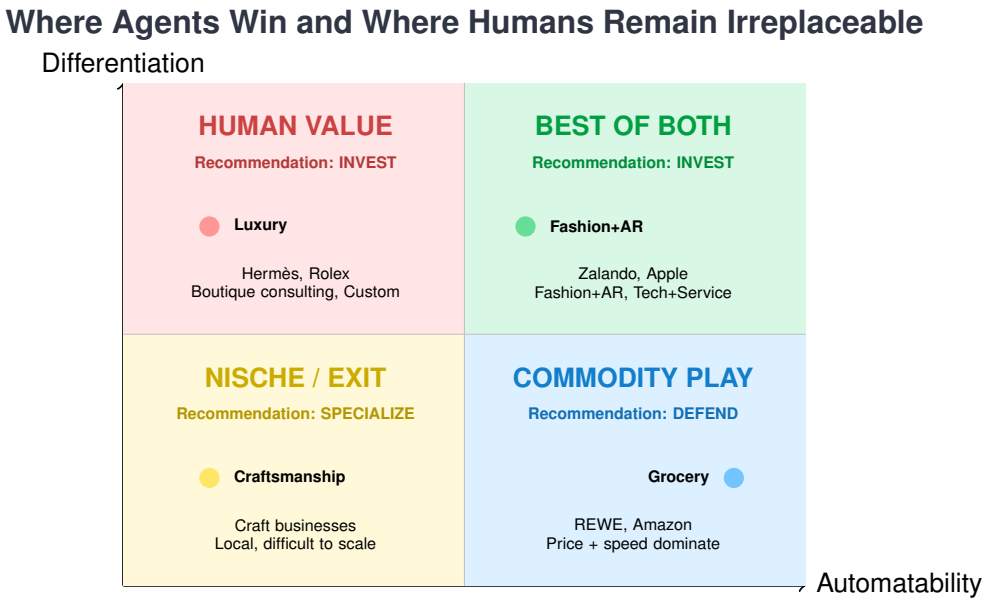

Figure 7: Strategy Matrix: Where agents win (right) and where humans differentiate (top). **INVEST** = build resources. **DEFEND** = protect margins. **SPECIALIZE** = find a niche.

2.2 Automatability vs. Differentiation

Definition: Experience in Agentic Commerce

Experience is not a feature, but a systemic operating system for decisions and trust:
Experience = Decision-making capability + Trust + Emotion

- **Decision-making capability:** Reduction of complexity through the structured presentation of options, comparisons, and consequences
- **Trust:** Orchestration of quality signals, reviews, certificates, and merchant reputation as tangible security
- **Emotion:** Sensory and identity-building experiences that agents cannot replicate

Important: AR, VR, and 3D are output channels for experience, not experience itself. Experience operates on three levels: for agents (machine-readable signals via AXP), for humans (immersive interfaces), and for hybrid scenarios (agent-assisted shopping).

2.3 Emotional Value Zones

Areas where human experience enables differentiation:

1. **Sensory Experiences:** Touch, smell, fit—not digitizable. Agents can provide product descriptions, but the tactile experience, the smell of leather, or the fit of a pair of jeans remain human domains. Merchants who offer showrooms, fitting rooms, or sample programs create uncopyable differentiation. *Important:* AR and VR are amplifiers of these experiences, not the differentiation itself—they reduce uncertainty but do not replace the physical experience.
2. **Identity-Building Purchases:** Luxury, gifts, custom products—the "why" matters more than the "what." Agents optimize for efficiency and price, but emotional purchases (gifts, mementos, status symbols) need human advice and storytelling. Merchants who understand

and communicate the personal significance of purchases win.

3. **Community:** Fans, collectors, belonging—not generatable by agents. Communities arise from shared passion, events, exclusivity. Agents can give recommendations but cannot create true belonging. Merchants with active communities (collector clubs, VIP programs, events) build sustainable moats.
4. **Serendipity:** Surprise, discovery—agents optimize for the known. Algorithms show what is similar. Humans discover by chance, through browsing, through personal recommendations. Merchants who offer curation, personal styling, or unexpected combinations create added value that agents cannot replicate.
5. **Expertise and Consulting:** Complex products need human expertise. Technical consulting, medical devices, B2B solutions—here, trust in human competence counts. Agents can provide data but cannot build a real consulting relationship.

Strategic Implication: Emotional Value Zones are not a niche—they are the differentiation in an automated market. Merchants should systematically identify: which parts of my business can agents not replicate? Expand these areas, don't reduce them.

Thesis: Emotional Value Zones

Automation makes human strengths more valuable. Merchants who identify and expand their Emotional Value Zones remain differentiated. Agents take over standard purchases—this makes human experiences more valuable, not superfluous.

Case Study: Best Practice: Shopware Spatial Commerce & Digital Sales Rooms

While agents take over the transaction ("buying"), the merchant must redefine the experience ("shopping"). With **Spatial Commerce** and **Digital Sales Rooms**, Shopware has created tools that agents cannot replicate:

- **Human Connection:** Video-based consulting in the Digital Sales Room builds trust for high-value products. An agent can provide data but cannot build a real human connection.
- **3D/Spatial:** Products become tangible in 3D (Apple Vision Pro, Meta Quest). This data is referenced via AXP (Agentic Experience Protocol) but is only actually *experienced* in the shop.
- **Configurator Experiences:** Complex product configurators (furniture, vehicles, fashion) offer interactive experiences that go beyond pure data queries.

Takeaway: Use agents for the logistics of the purchase, but Shopware features for the emotion of the decision. The combination is the competitive advantage.

Actionable Recommendation: What you do differently now

This week:

- Extend customer journey map to include agent touchpoints
- **First artifact:** New journey map with 5 agent phases

Next 14 days:

- Human Value Audit: Identify your 3 strongest non-automatable experiences
- **Responsibility:** Product + Marketing together

Next 30 days:
- Start AR/3D pilot in a category with high sensory demand

Implications by Target Group – Part I

If you are a Merchant:

- Disruption affects your distribution—not your product
- Invest in data quality (UCP), not in more ads
- Identify your Human Value Islands as differentiation
- **No-Go:** Do not ignore agent channel readiness—it is existential

If you are a Platform:

- Your gatekeeper position is transforming into a protocol or trust layer
- Open standards (UCP, AXP) are strategically more important than proprietary APIs
- Position yourself as an enabler, not a bottleneck
- **No-Go:** Do not block agent access—this accelerates disintermediation

If you are an Investor:

- The value shift is moving from traffic to protocols and trust
- Protocol-capable merchants are better positioned than SEO-dependent ones
- Experience tech (AR/3D/AXP) is a differentiation lever, not a nice-to-have
- **No-Go:** Do not evaluate companies based on old e-commerce KPIs—agent adoption is more relevant

PART II

Operational Implications

3 Operating Model 2030

If you skip this chapter: You start agent integrations without clear ownership. The result: finger-pointing between IT, marketing, and operations. And in the end, the integration fails because of internal silos, not technology.

3.1 New Roles and Systems

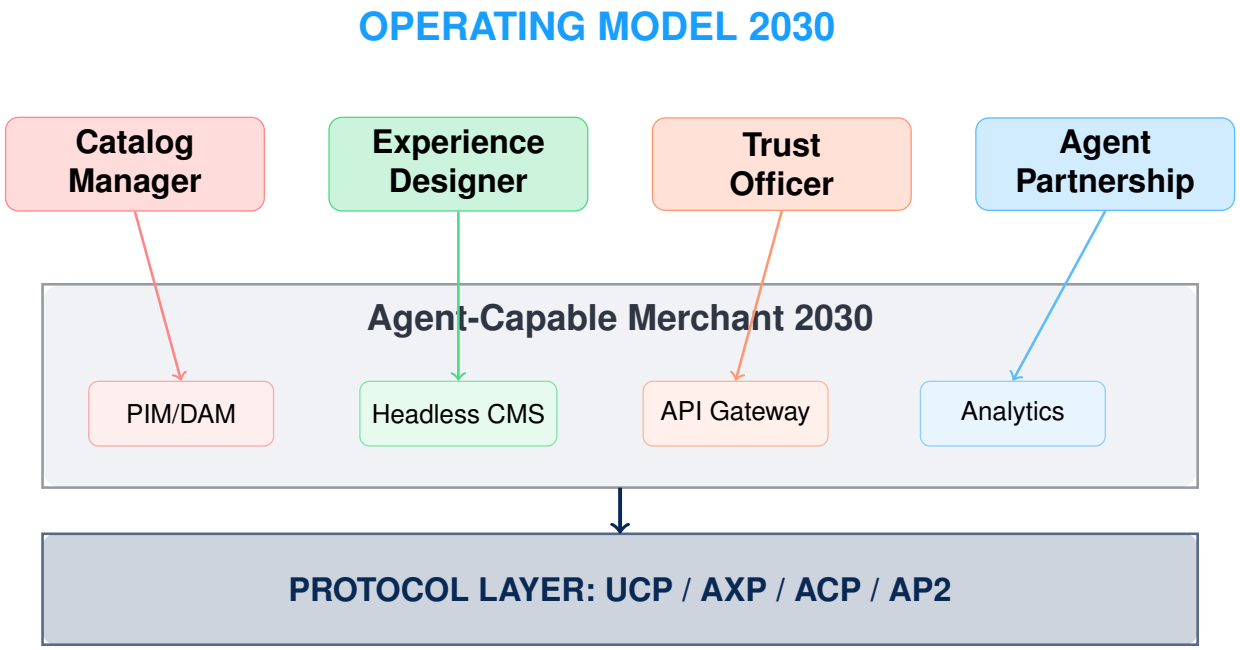

Figure 8: Operating Model 2030: Four core roles (top) manage specialized systems (middle), which communicate with agents via the common protocol layer (bottom).

Experience Role: Core Tasks

The Experience role is *not* content management, but Decision Design. The tasks:

- **Decision Reduction:** Designing comparisons, filters, and recommendation logic that reduce complexity for users and agents
- **Trust Presentation:** Displaying quality signals, reviews, and certificates as tangible security (not just as data points)
- **Human Handovers:** Defining thresholds and triggers for when agents escalate to humans (e.g., for high-value purchases, customization, need for consulting)
- **Experience Embedding:** Technical integration of 3D, AR, and configurators via AXP into agent surfaces—with clear sandbox boundaries

Distinction: Experience is *not* marketing (brand campaigns), *not* IT (API infrastructure), and *not* support (after-sales). Experience designs the moment of decision.

3.2 RACI Matrix

KPI/Task	Catalog	Experience	Trust	Agent Partnership
Data Fill Rate	**R/A**	C	I	I
Experience Coverage	C	**R/A**	I	I
Trust Score	I	C	**R/A**	I
API Uptime	I	I	C	**R/A**
Agent Adoption	I	C	C	**R/A**
Decision Flow Design	I	**R/A**	C	C
Trust Signal Presentation	I	**R/A**	C	I
Human Handover Definition	I	**R/A**	C	C
Experience Policy Compliance	I	C	**R**	**A**

Table 5: RACI Matrix: R=Responsible, A=Accountable, C=Consulted, I=Informed. This matrix shows responsibilities—so you can identify ownership gaps.

3.3 KPIs per Role (Detail)

Role	Top-3 KPIs	Target Value	Frequency
Catalog	Data Fill Rate, Update Speed, Schema Compliance	**>95%**, <5 min, 100%	Daily
Experience	Decision Completion Rate, Assisted Conversion Rate, Human Handover Rate, Embedding Rate	>85%, >15%, <8%, >10%	Weekly
Trust	Trust Score, Policy Abort Rate, Incident Resolution	**>75**, <5%, <4h	Daily
Agent Partnership	Agent Adoption, Conversion Rate, New Integrations	>20%, **>3%**, 2+/Q	Weekly

Table 6: KPIs per Role. This table shows what each role must measure—so you can detect performance problems early.

New Experience KPIs Explained:

- **Decision Completion Rate:** Percentage of sessions in which users/agents make a purchasing decision (do not cancel). Measures decision reduction.
- **Assisted Conversion Rate:** Percentage of conversions where agent experience components (comparisons, trust signals) were used. Measures experience impact.

- **Human Handover Rate:** Percentage of agent sessions escalated to humans. Too high = poor decision UX. Too low = missed margin opportunities.
- **Embedding Rate:** Percentage of sessions with rendered experience components (3D, AR). Still relevant, but no longer the only KPI.

3.4 Anti-Patterns and Misconceptions

Risk: Typical Organizational Errors

Anti-Pattern 1: Catalog = PIM only
Misconception: "We have a PIM, so our data is agent-ready." Reality: PIM data is often not UCP-compliant. **Solution:** Dedicated Catalog role with schema validation.
Anti-Pattern 2: Trust as a Support Task
Misconception: "Trust is a customer service topic." Reality: Trust Score directly influences agent decisions. **Solution:** Trust as a separate role with KPI responsibility.
Anti-Pattern 3: Experience = Marketing
Misconception: "3D and AR belong to marketing." Reality: Experience embedding is technical integration. **Solution:** Cross-functional team of marketing + dev.
Anti-Pattern 4: Agent Partnership = IT Project
Misconception: "API connectivity is an IT matter." Reality: Agent Partnership is business development. **Solution:** Dedicated role with P&L responsibility.

3.5 Moat Evaluation Matrix

Moat	Setup Cost	Time	Metric	Risk
Trust Excellence	Medium	12–24 mo	Trust Score	Incident erosion
Community IP	High	24–36 mo	Member count	Platform lock-in
Experience IP	Medium-High	6–12 mo	Embedding rate	Tech obsolescence
Exclusive Bundles	Low	3–6 mo	Bundle AOV	Ease of copying
Returns Excellence	Medium	6–12 mo	Return NPS	Cost explosion

Table 7: Moat Evaluation: Effort, time, measurement, and risks.

Hypothetical Scenario: Transformed Fashion Merchant

Hypothetical example: A medium-sized fashion merchant restructures: 3 Catalog, 4 Experience, 2 Trust, 2 Agent Partnerships. *Assumption after 12 months:* Significant agent channel share at higher AOV. *Measurement:* Order attribution via UTM + API header.

Actionable Recommendation: What you do differently now

This week:

- Org Check: Are the four roles (Catalog, Experience, Trust, Agent Partnership) filled?
- **First artifact:** Org chart overlay with the four roles

Next quarter:

- Implement top-3 KPIs per role (see KPI chapter)
- **Responsibility:** COO or VP Operations

Immediately:

- Anti-Pattern Audit: Do you fall into any of the four patterns? (Catalog=PIM, Trust=Support, etc.)

4 Agent Negotiation and Policy Files

If you skip this chapter: Agents will negotiate your prices down without you even noticing. Systematically, across thousands of products, 24/7. Without policies, you are at their mercy.

Definition: Policy Files as Alliance Proposal

Status: Policy Files are a **recommended pattern** (Alliance Proposal), not a standardized format. AP2 describes mandates and audit trail as core mechanics. Visa TAP addresses agent verification. The policy JSON format described here is a compatible extension that brings these concepts together.

4.1 The Control Problem

When agents buy on behalf of users, a fundamental control problem arises: how do you ensure that agents act not only efficiently but also **profitably and with minimized risk**? Without clear rules, agents can push prices down, close unprofitable deals, or even enable fraud.

Policy Files solve this by defining machine-readable guidelines that agents must check and respect in advance. They integrate seamlessly into AP2 (Mandates) and Visa TAP (Agent Identity).

4.2 Why Policies are Economically Important

Policies are not just technical hurdles—they are the **core of your margin protection strategy**. Imagine: an agent negotiates for a customer across thousands of products and systematically looks for discounts. Without policies, this could lead to an erosion of your prices, as agents (e.g., via A2A protocols) could exchange information with each other.

Economically speaking, policies protect your take rates: in scenarios with high agent adoption, they prevent merchants from being degraded to mere price suppliers.

Policy Files are the equivalent of pricing, discount, and channel governance in the age of agents. They define not only security but also market positioning relative to machines.

4.3 Policy Types

- **Pricing:** Minimum prices, discount limits, dynamic adjustments
- **Availability:** Stock levels, delivery times, fallback options
- **Returns:** Return periods, conditions

- **Identity:** Verifiable credentials via AP2 for fraud prevention
- **Geo:** Regional restrictions
- **Fraud:** Risk scores, thresholds, human approval for high-value purchases

4.4 Policy File Concept (Alliance Proposal)

Note: This concept is an Alliance Proposal, not an adopted standard. It shows how machine-readable merchant policies could work together with AP2 Mandates and Visa TAP Agent Identity.

Core Idea:

- Merchants must enforce policies server-side
- Agents receive machine-readable reasons for rejection
- Optionally, there can be a discovery manifest for this

Possible Discovery: An obvious location would be `/.well-known/...` in the sense of RFC 8615. The final path is part of a possible standardization. Alternatively, policy discovery can be transported as a UCP Capability.

Security: Policies should be signed (e.g., via JWS in `application/jose+json` format) and support TTL-based caching.

Example Rule Categories:

```
{
  "policy_version": "1.0.0",
  "merchant": "example-shop.com",
  "policies": {
    "max_discount_percent": 20,
    "min_order_value_eur": 10,
    "geographic_restrictions": ["DE", "AT", "CH"],
    "agent_identity_required": true,
    "human_approval_threshold_eur": 500
  }
}
```

Important: Internal calculation data (such as margins) should not be exposed. Policies define limits for agents, not business secrets.

4.5 Threat Model: Attack Vectors and Controls

Policy Files must be protected against various attack vectors:

1. **Price Scraping plus Cart Stuffing:** Agent systematically collects prices and exploits price differences. *Control:* Rate limiting, agent identity verification via Visa Trusted Agent Protocol.
2. **Credential Forgery:** Forged agent credentials enable mass purchases. *Control:* Verifiable credentials in AP2, WebPKI, or DNS-based verification.
3. **Replay Attacks:** Old policy versions are reused. *Control:* TTL enforcement, versioning with Semantic Versioning.

4. **Prompt Injection via Product Content:** Agent interprets product descriptions as instructions. *Control:* Structured data only, schema validation via UCP/AXP.
5. **Fraud via Mandate Manipulation:** Manipulated mandates bypass budget limits. *Control:* AP2 mandate logic with audit trail, human approval at thresholds.

4.6 Enforcement: What Happens on Policy Violation

If a policy is violated, the process is aborted—the agent must either adjust or cancel. In the worst case: blacklisting of the agent.

Figure 9: Policy Discovery Flow: Fetch, Validate, Apply with three end nodes (Accept, Reject, Fallback).

Risk: Policy Gaps

Without robust policies, you risk margin erosion and fraud. Implement at least pricing and identity policies before agent launch.

Actionable Recommendation: What you do differently now

Today:
- Policy Audit: Does `/.well-known/agent-policy.json` exist? If not: create it.
- **First artifact:** Minimal policy file with pricing rules

This week:
- Threat Assessment: Evaluate risks for price scraping and credential forgery
- **Responsibility:** Security + Commerce together

Next 14 days:
- Define human approval thresholds (e.g., >500 EUR = manual)

5 The Agentic Commerce Alliance

If you skip this chapter: Standards will be set without you. You will later implement what others define today—on their terms.

The Agentic Commerce Alliance (https://www.agentic-commerce.org) is the central industry initiative for open standards in Agentic Commerce. Founded in July 2025 under the leadership of Shopware, it brings together merchants, technology providers, payment providers, and AI companies worldwide.

5.1 Mission: Human Value Preservation

The Alliance was born out of a strategic necessity: without open standards, there is a threat of a scenario where a few big tech platforms control all agent commerce. The mission of the Alliance:

1. **Open Standards:** Development and maintenance of protocols (UCP, AXP, AP2) that are not controlled by individual companies
2. **Merchant Sovereignty:** Ensuring that merchants remain the Merchant of Record and that customer data does not flow to platforms
3. **Interoperability:** Avoiding lock-in through compatible protocols across all agent surfaces
4. **Emotional Value Zones:** Protection and promotion of areas where human interaction creates added value

5.2 Protocol Governance

5.3 Shopware as a Founding Member

Shopware plays a central role as a founding member:

- **AXP Development:** Primarily responsible for the Agentic Experience Protocol
- **Reference Implementations:** SwagUcp plugin for Shopware 6 (Open Source)
- **Spatial Commerce:** Integration of 3D/AR experiences via AXP
- **PayPal StoreSync:** Deep integration as a platform partner

Actionable Recommendation: Join the Alliance

Merchants and technology providers can join the alliance at https://www.agentic-commerce.org/join. Benefits: contributing to standards, early access to protocol updates, networking with industry leaders.

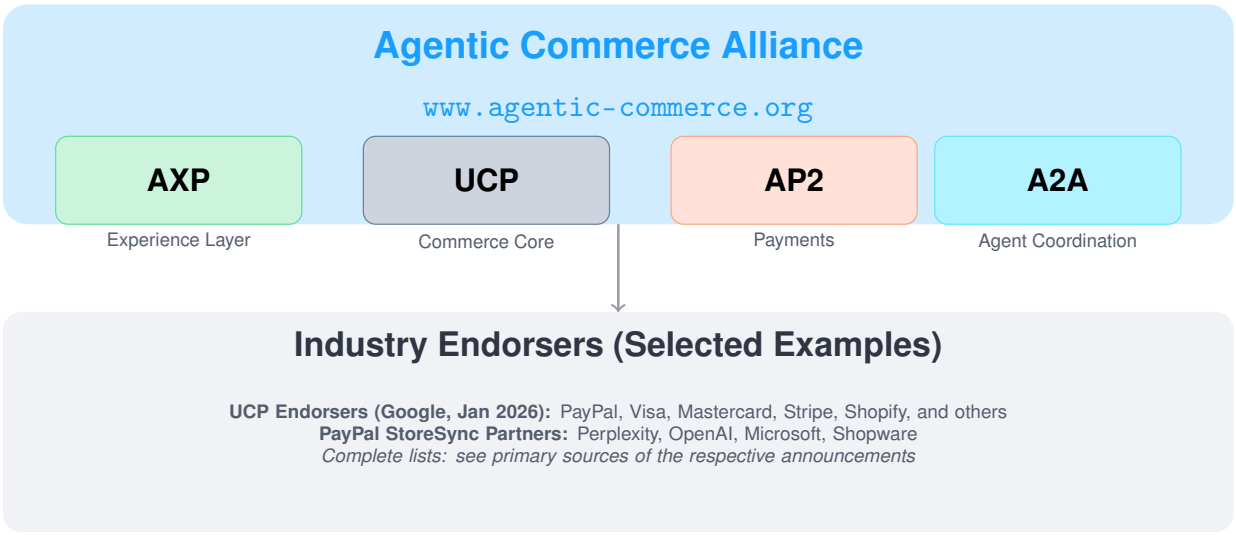

Figure 10: Agentic Commerce Alliance: Protocol Governance and Industry Partners.

Implications by Target Group – Part II

If you are a Merchant:

- Your organization needs the four roles: Catalog, Experience, Trust, Agent Partnership
- Policy Files are margin protection, not bureaucracy—implement them before agent launch
- Measure the new KPIs: Agent Adoption, Trust Score, Policy Abort Rate
- **No-Go:** Do not treat Agent Partnership as an IT project—it is business development

If you are a Platform:

- Support merchants in building the four roles with tools and templates
- Policy infrastructure is strategic—offer simple Policy File generation
- Integrate KPI dashboards for agent metrics into your analytics
- **No-Go:** Do not delay Alliance participation—standards are being set now

If you are an Investor:

- Due diligence must query the operating model for Agentic Commerce
- Portfolio companies need policy readiness and KPI tracking
- Alliance membership is a positive signal for protocol readiness
- **No-Go:** Do not invest in companies that categorize the agent channel as "later"

PART III

Technology & Strategy

6 Protocol Roadmap Q1 2026

If you skip this chapter: You make build-vs-buy decisions blindly. You build what you should buy and buy what you should build. Both will cost you 6–12 months.

This chapter provides an overview of the current protocol landscape in Agentic Commerce. Important: No protocol replaces another. They address different layers of the same agentic purchasing process and together form an interoperable Agentic Commerce stack with complementary protocols.

6.1 The Master Stack Diagram

This diagram is the central reference for all protocol discussions in this strategy book. All subsequent chapters refer to these five layers.

6.2 Level 1: Core Commerce

UCP (Universal Commerce Protocol): An end-to-end commerce protocol for discovery, capability description, order, and checkout orchestration. Launched as an open standard by Google (January 11, 2026) and endorsed by more than 20 others. It defines an open, common language for agents, merchant backends, platforms, and payment services across the entire purchasing process—from discovery and ordering to post-purchase. It is compatible with AP2 (payment mandates), A2A (agent-to-agent communication), and MCP (context/data transport).

ACP (Agentic Commerce Protocol): An open, productively used checkout standard for agentic purchase conclusions (Instant Checkout). Licensed under Apache 2.0 and maintained by OpenAI and Stripe. Optimized for agent-driven checkout flows with shared payment tokens and a Merchant of Record model. It forms the basis for OpenAI Instant Checkout in ChatGPT and is referenced by Microsoft as an "open standard."

6.3 Level 2: Payments & Trust

AP2 (Agent Payments Protocol): A standard for payment mandates and secure, cryptographically verifiable agent payment authorization. Documented by Google as an open Agent Payments Protocol. It defines payment mandates and authorization for agent transactions and is compatible with UCP, intended for UCP flows.

Visa Trusted Agent Protocol (TAP): Introduced by Visa (October 14, 2025). It addresses agent identity, consumer recognition, and payment information. It complements other protocols like ACP

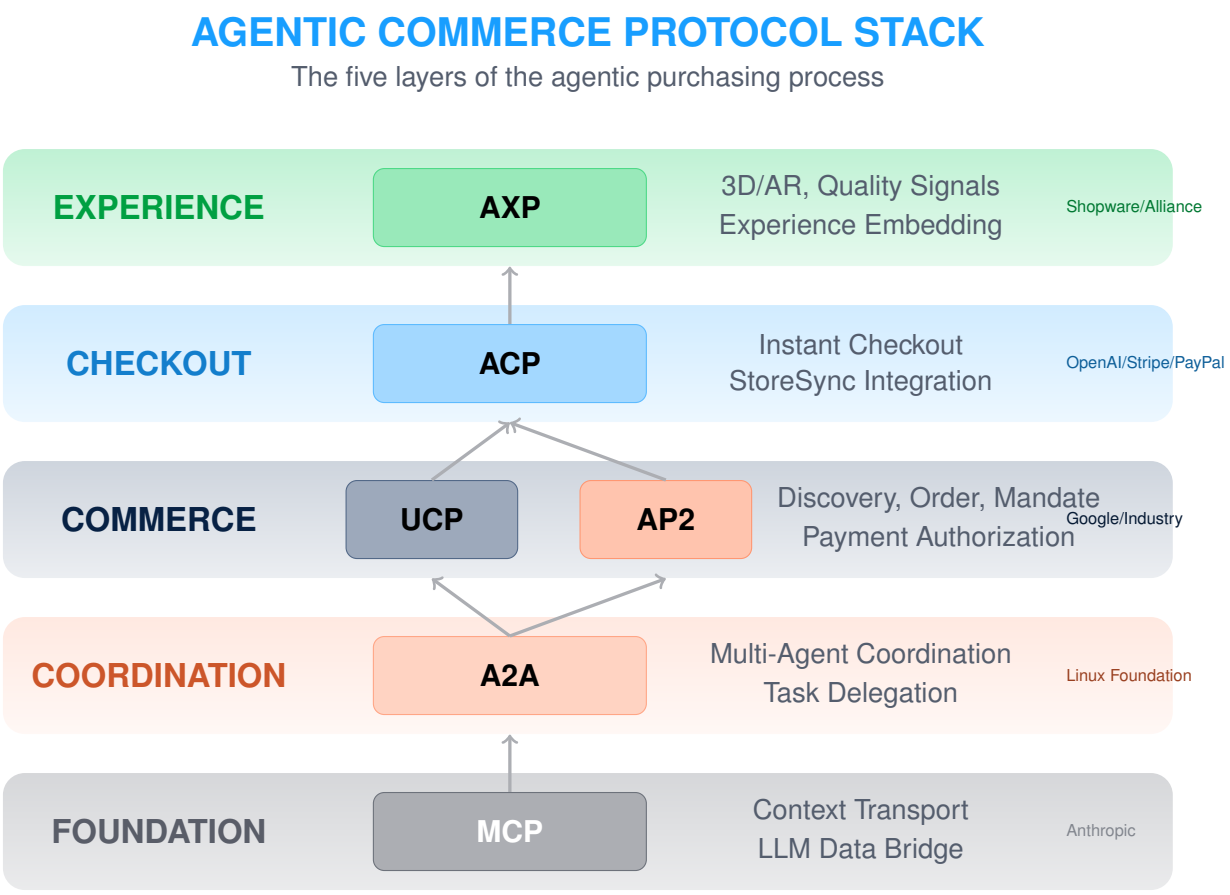

Figure 11: Master Stack Diagram: The five layers of Agentic Commerce. MCP as the integration layer, building up to A2A (Coordination), UCP/AP2 (Commerce), ACP (Checkout), and AXP (Experience). This diagram is the central reference.

and AP2 in the trust layer.

6.4 Level 3: Agent Coordination & Context

A2A (Agent2Agent Protocol): Enables multi-agent scenarios and agent-to-agent communication. Used by UCP for complex orchestrations.

MCP (Model Context Protocol): Basic context transport for agent communication, production-ready. Enables context/data transport between agents and services.

6.5 Level 4: Experience Layer

AXP (Agentic Experience Protocol): Developed by Shopware and the Agentic Commerce Alliance. It extends UCP with three core capabilities:

1. **Product Data:** Structured product information for complex types (variants, configurators, events, subscriptions, bundles)
2. **Quality Data:** Trust signals including reviews, returns, intent information, and merchant reputation
3. **Experience Embedding:** Sandboxed live experiences from merchants (3D viewers, configu-

rators, AR)

AXP Capabilities:

- `dev.axp.product_data` – Basic product data
- `dev.axp.product_data.variants` – Variant support
- `dev.axp.product_data.configurator` – Complex configurators
- `dev.axp.quality_data.reviews` – Reviews and ratings
- `dev.axp.quality_data.trust` – Merchant and product trust
- `dev.axp.experience_embedding.viewer_3d` – 3D viewer
- `dev.axp.experience_embedding.ar` – Augmented Reality
- `dev.axp.decision_metadata` – Structured decision support (comparisons, filters, recommendation logic)
- `dev.axp.trust_presentation` – Trust signal presentation instructions for agent surfaces
- `dev.axp.escalation_hooks` – Human handover triggers and escalation thresholds

Important: AXP is not just a media protocol for 3D/AR, but a comprehensive experience transport system. The new capabilities (`decision_metadata`, `trust_presentation`, `escalation_hooks`) allow merchants to provide decision logic and trust orchestration as machine-readable hints, not just as visual assets.

Deployment: AXP can be deployed as a UCP addon (`/.well-known/ucp`) or standalone (`/.well-known/axp`).

Policy Files: Machine-readable guidelines at `/.well-known/agent-policy.json`, integrating with ACP and AP2. They define pricing, discount, and channel governance in the age of agents.

6.6 Level 5: Commerce Enablement Services

PayPal StoreSync: PayPal's flagship service for Agentic Commerce. It makes merchant product data findable in leading AI channels and orchestrates the entire cart lifecycle.

StoreSync Components:

- **Product Feed Integration:** Automatic synchronization of product catalogs. Near-real-time inventory, pricing, and attributes. Supports Google Shopping CSV format.
- **Cart Orchestration:** Complete shopping journey from discovery to checkout. AI agents can create carts, apply coupons, and handle shipping options.
- **Headless Checkout:** Integration with any AI surface without redirect.

StoreSync Partners:

- **AI Surfaces:** OpenAI (ChatGPT Instant Checkout), Microsoft (Copilot Checkout), Perplexity (Instant Buy), PayPal App Shopping Agent
- **Platforms:** Shopware, Wix, Cymbio, BigCommerce/Feedonomics

Merchant Value: Merchants remain the Merchant of Record, retain customer contact, and maintain brand visibility. A PayPal integration enables presence on all AI surfaces.

Experience Embedding: Security and Compliance Boundaries

AXP Experience Embedding (3D, AR, configurators) follows strict security guidelines:

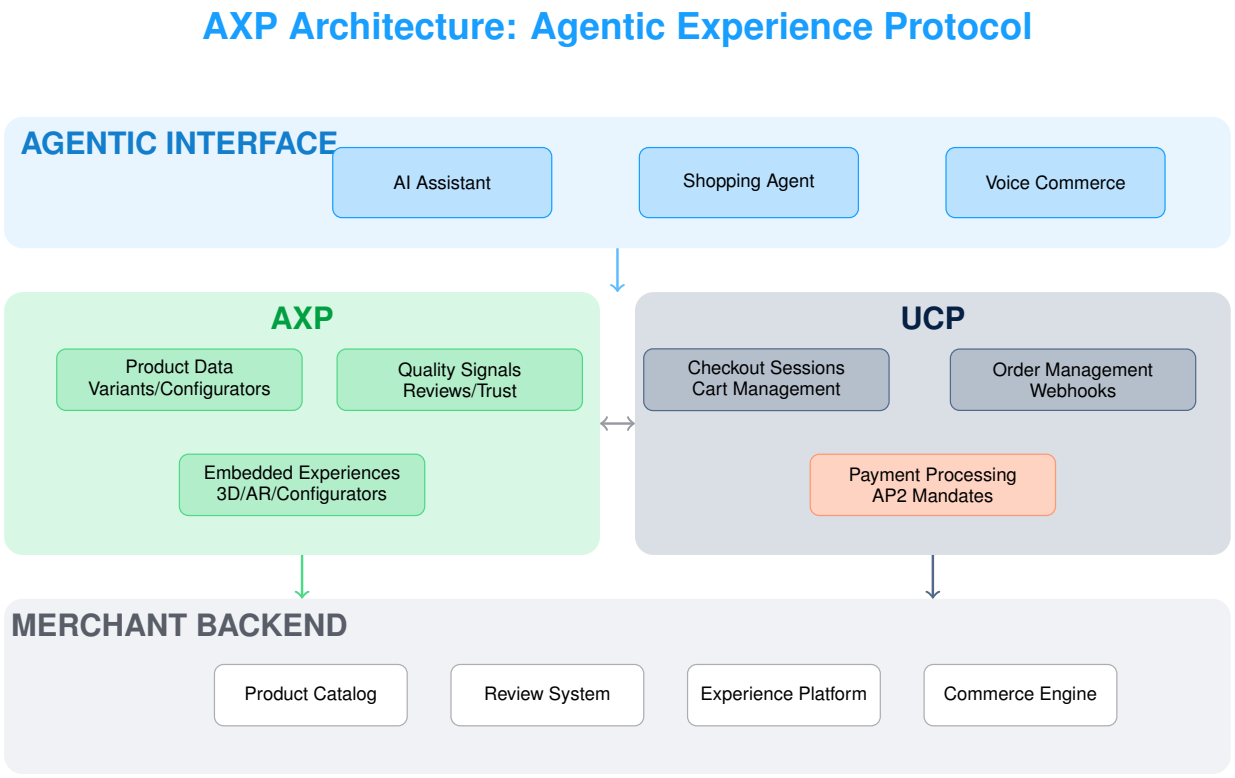

Figure 12: AXP Architecture: The Agentic Experience Protocol extends UCP with structured product data, quality signals, and embedded experiences. Both protocols communicate via standardized interfaces.

- **No Full Page Takeover:** Embedded experiences must not take over the entire agent interface. Maximum viewport area: 60% (recommended).
- **No Uncontrolled Scripts:** Sandboxed execution via iframe with Content Security Policy (CSP). No access to agent context or user data outside the embedding.
- **Deterministic UX Boundaries:** Clear demarcation between agent interface and merchant embedding. The user must be able to recognize at all times who controls which part.

Rationale: These boundaries protect users from phishing, fraud, and dark patterns. They allow merchants to offer differentiated experiences without putting agent platforms at liability risk. Compliance teams and security officers can confidently approve experience embedding.

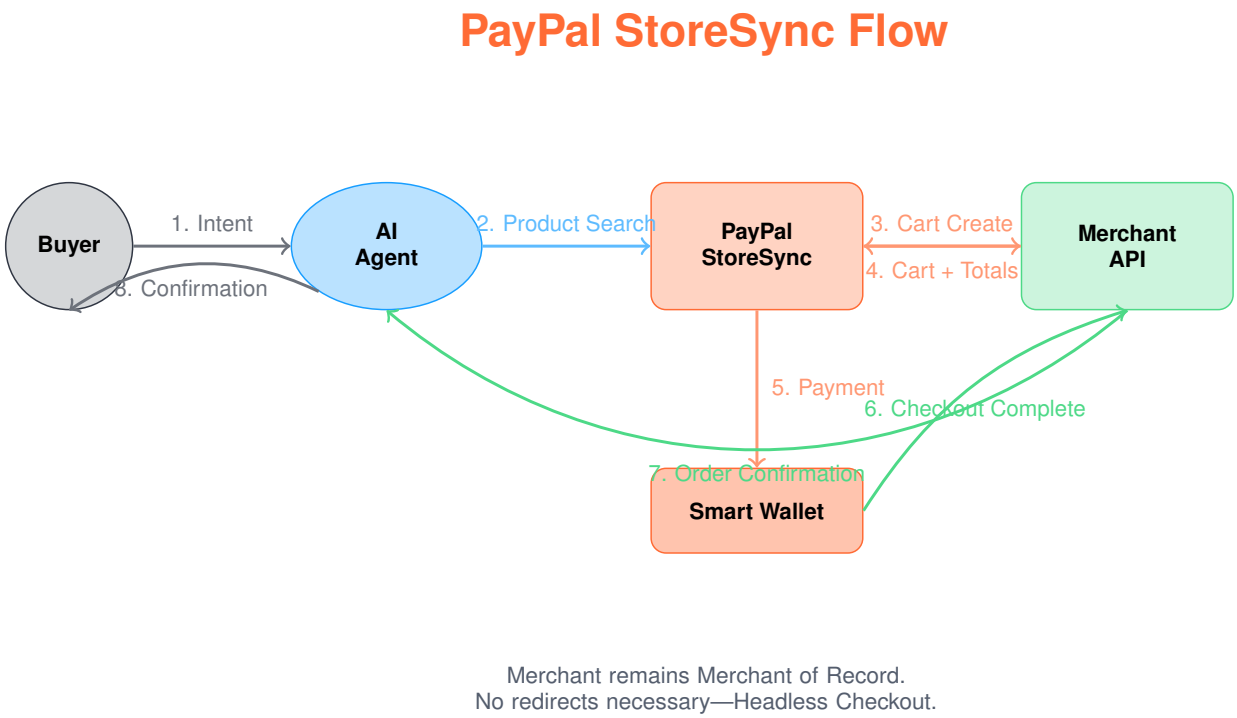

Figure 13: PayPal StoreSync Flow: From Buyer Intent to Order Confirmation. The agent communicates with PayPal StoreSync, which handles cart orchestration. Smart Wallet enables seamless checkout without redirects.

7 The Agentic Commerce Tech Stack

7.1 Protocol Stack: Detail View

The protocols form an interoperable stack with clear layering (see Master Stack Diagram on page 31). Each layer addresses specific requirements of the agentic purchasing process:

- **Foundation (MCP):** Basic context transport between LLMs and external data sources
- **Coordination (A2A):** Multi-agent scenarios and task delegation
- **Commerce (UCP/AP2):** Discovery, order management, and payment authorization
- **Checkout (ACP):** Instant checkout flows and StoreSync integration
- **Experience (AXP):** 3D/AR, quality signals, and experience embedding

7.2 Protocol Overview

Note on Architecture: The protocols together form an interoperable stack. UCP orchestrates the entire commerce flow, including purchase and order management. AP2 is intended as a compatible payments layer. ACP is an alternative checkout implementation (OpenAI/Stripe). A2A and MCP are additions for agent coordination and context transport.

Protocol	Function	Econ. Significance	Status Q1/26
UCP	End-to-end commerce incl. checkout	Standardization reduces costs	Initial Release[1]
ACP	Instant Checkout (Alternative)	Fast checkout integration	Draft (Spec)[2]
AP2	Payment mandates & authorization	Secure agent payments	Initial Release[3]
Visa TAP	Trust & Identity	Agent verification	Available[4]
A2A	Agent coordination	Multi-agent scenarios	Early Adoption
MCP	Context transport	Basic agent communication	Productive[5]
AXP	Experience Layer	Rich content in agents	Alliance Proposal

Table 8: Protocol Status Q1/2026. **Available** = Specification published, first implementations. **Initial Release** = Published specification. **Draft** = Specification in development.

7.3 Two Checkout Paths in Agentic Commerce

Google describes UCP as the standard for the entire commerce journey, including purchase and order management. ACP (OpenAI/Stripe) focuses on Instant Checkout. Both approaches exist in parallel in the market:

Aspect	Path 1: UCP + AP2 (Google)	Path 2: ACP (OpenAI/Stripe)
Scope	End-to-end: Discovery to Order	Focus: Instant Checkout
Payment	AP2 Mandates integrated	Shared Payment Tokens
Endorsers	Google, PayPal, Visa, 20+ partners	OpenAI, Stripe, Microsoft
Best for	Full-stack integration	Fast checkout launch

Table 9: Two dominant checkout variants. You don't have to choose—both are compatible and can be implemented in parallel.

7.4 How an Agent Buys: Sequence Diagram

Note: The protocols work together in an interoperable stack. UCP orchestrates the entire flow, AP2 secures payment authorization, and ACP enables instant checkout flows.

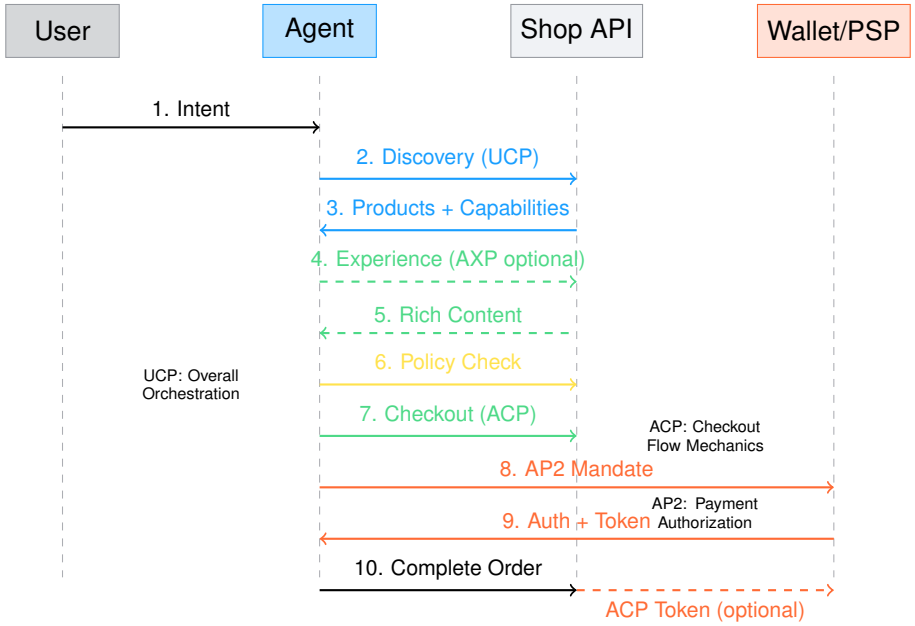

Figure 14: Purchasing process in the interoperable protocol stack with optional branches.

7.5 In-house Development vs. Partner

Component	In-house Development	Partner
UCP Integration	Only for very specific needs	Recommended: Platform plugins
Agent Gateway	For >10 agent integrations	Recommended: StoreSync or similar
Experience Engine	For unique UX visions	3D: Various providers
Trust Aggregation	Rarely useful	Mostly partners

Table 10: In-house Development vs. Partner: Recommendations.

8 Experience Platform

If you skip this chapter: You will become a commodity. Agents will only compare you based on price and delivery time. Your brand, your content, your UX—invisible to agents.

The experience platform is the differentiator in Agentic Commerce: while agents automate standard purchases, merchants win through structured decision aids, trust orchestration, and immersive experiences. Based on the Agentic Experience Protocol (AXP), it transports not just rich content but the entire Decision and Trust Operating System.

8.1 Why Experience Platforms are Crucial

Agents optimize for efficiency, but decisions need structure and trust. Experience platforms act on three levels:

- **Decision Experience:** Structured comparisons, filters, and recommendations reduce complexity for agents and humans
- **Trust Experience:** Presentation of quality signals as tangible security, not just data points
- **Immersive Experience:** 3D viewers, AR, and configurators for sensory and emotional differentiation

Important: Most merchants start at Level 3 (Immersive), even though Level 1 (Decision) and Level 2 (Trust) deliver value faster and are cheaper to implement.

Conversion Uplift through Experience Embedding:

15–25% *(Scenario based on AR benchmarks and pilot projects)*

- **Baseline:** Conversion rate without experience embedding (agent orders, category-specific)
- **Segmentation:** Fashion, furniture, and electronics benefit more than commodities
- **Critical Factor:** Load time <2s, otherwise latency kills the effect
- **Measurement:** A/B test with/without embedding, attribution via UTM + API header

The core question: **What can an agent not deliver alone?** The answer: sensory, emotional, and identity-building experiences.

8.2 Concrete Patterns

AR Viewer: Users "try on" products virtually—furniture in the room, glasses on the face. In AXP: sandboxed embedding.

3D Configurator: Customers build products themselves. Real-time pricing via AXP.

Guided Selling: Agent-guided consulting with preference matching.

Community Loops: User-generated content in AXP Quality Data.

Service Bundles: Purchases with add-ons: installation, warranty.

Returns as Trust Lever: Simulated returns via AXP build trust.

Actionable Recommendation: Building an Experience Platform

This week: Choose a category with high sensory demand (fashion, furniture, electronics).
Next 30 days: AR pilot live, measure embedding rate.
Target Q1: 10% embedding rate, first conversion data.
Responsibility: Experience team (not marketing alone).

Actionable Recommendation: What you should decide differently now

- **Category Selection:** Identify the category with the highest experience potential
- **Tech Stack:** Evaluate 3D/AR providers for AXP compatibility
- **Measurability:** Define embedding rate and conversion uplift baseline before pilot start

9 KPIs in Agentic Commerce

If you skip this chapter: You continue to measure conversion rate and page views, while the real levers—Agent Adoption, Trust Score, and Policy Abort Rate—remain in the dark. You are steering with outdated instruments.

9.1 KPI Definitions with Formulas

KPI	Formula/Definition	Frequency	Responsible
Data Fill Rate	Mandatory fields / Total $\times$ 100	Daily	Catalog
Update Speed	Median(sync time) in minutes	Real-time	Catalog
Agent Adoption	Agent orders / All orders $\times$ 100	Weekly	Agent Partnership
Agent Conversion	Agent-completed / Agent-initiated	Weekly	Agent Partnership
Trust Score	Trust Index 0–100	Monthly	Trust
Policy Abort Rate	Abortions / Agent requests	Real-time	Trust

Table 11: KPI Definitions: This table shows the six core KPIs—so you know what you need to measure to manage agent readiness.

Definition of Agent Order: An order initiated by an agent using standardized agent credential headers/tokens (verified agent identity). Recommendation: Mark agent orders via standardized request metadata, for example, signed agent credentials or gateway headers. The field name is an implementation detail (e.g., `X-Agent-ID` header or agent referrer).

9.2 KPI Implementation: Stack Signal and System of Record

Practical Notes:

- **Multi-agent scenarios:** In A2A flows, one order can involve multiple agents. Attribution to the initiating agent via $\texttt{primary}_{a}gent_{i}d$.
- $\texttt{Retry handling: AP2 mandates are idempotent. Use mandate}_{i}dasthededuplicationkey$.
- `Cross-system sync: Trust Score aggregates from multiple sources (reviews, returns, incidents). Define clear update frequencies and conflict resolution.`

KPI	Stack Signal	System of Record	Deduplication
Agent Adoption	AP2 Mandate Event	Order system	Idempotency key per mandate
Trust Score	AXP Quality Signals	Trust aggregator	Timestamp + source
Policy Abort	Policy Gateway Event	Gateway logs	Request ID + session
Data Fill Rate	UCP Schema Validation	PIM/DAM	SKU + timestamp
Update Speed	UCP Sync Event	API Gateway	Event ID + retry counter
Agent Conversion	ACP/UCP Checkout Event	Order system	Session ID + agent ID

Table 12: KPI Implementation: Mapping protocol signals to backend systems.

Actionable Recommendation: What you do differently now

This week:
- Add Agent Adoption and Trust Score to the exec dashboard
- **First artifact:** Dashboard widget with two new KPIs

Next 14 days:
- Implement agent order tracking via `X-Agent-ID` header
- **Responsibility:** Engineering + BI together

Next 30 days:
- Alerts: Policy Abort Rate >5

9.3 Target Values by Category (Scenario)

KPI	Grocery	Fashion	Electronics	Luxury
Update Speed	**<1 min**	<30 min	<5 min	<60 min
Agent Adoption*	**70–80%**	40–50%	50–60%	10–20%
Trust Score	**80+**	70+	75+	60+

Table 13: Target values by category (Scenario 2030). *All values are illustrative assumptions based on automatability and category characteristics—not forecasts.

10 Strategic Roadmap

If you skip this chapter: You start without gates. You scale before the pilot works. Or you wait too long and miss the window where first movers still have an advantage.

10.1 Phases with Economic Gates

Phase	Timeline	Activities	Success Gate	Econ. Gate
Audit	Mo 1–3	Data audit, API check	Readiness score	Budget OK
Pilot	Mo 4–6	1 agent, 1 category, **Decision UX**	First orders	CAC neutral
Scale	Mo 7–12	Multi-agent, **Hybrid Experience**	20%+ agent	Margin stable
Optimize	Mo 13+	**Immersive Experience**, A/B	Profitability	CM positive

Table 14: Roadmap with economic gates: CAC, Margin, Contribution Margin.

Experience focus per phase:

- **Pilot Phase:** Decision UX—structured comparisons and decision aids without expensive AR production. Goal: establish conversion baseline.
- **Scale Phase:** Hybrid Experience—trust signal presentation and human handover triggers. Goal: assisted conversion rate >15%.
- **Optimize Phase:** Immersive Experience—3D, AR, and configurators for high-value categories. Goal: margin defense against standard providers.

Critical: Merchants who start immediately with AR skip Decision and Trust Experience. Result: high costs, but no conversion improvement because the decision logic is missing.

10.2 Capability Ladder

1. **Level 1 – Data Readiness:** Complete, UCP-compliant product data
2. **Level 2 – Trust Signals:** Reviews, certificates, and return policies in machine-readable format
3. **Level 3 – Agent Channels:** First API connections, policy files live
4. **Level 4a – Decision Experience:** Structured comparisons, filters, and decision aids via AXP Decision Metadata
5. **Level 4b – Trust Experience:** Trust signal presentation and human handover triggers via AXP Trust Presentation

6. **Level 4c – Immersive Experience:** AR, 3D, and configurators via AXP Experience Embedding
7. **Level 5 – Multi-Agent:** Orchestration of multiple agents, B2B scenarios

Important: Merchants do *not* have to start with Level 4c (AR/3D). Level 4a (Decision Experience) already delivers measurable value through better decision reduction—without expensive 3D production. Level 4b (Trust Experience) increases conversion through better trust presentation. Level 4c is the "nice-to-have," not the requirement.

11 Risks and Controls

Risks in Agentic Commerce are diverse but manageable. This chapter extends the risk-control matrix to include hypothetical incident patterns, specific controls, and liability issues.

11.1 Hypothetical Incident Patterns

Hypothetical Scenario: Hallucination Risk

Hypothetical example: An agent could "hallucinate" incorrect product availability, leading to overbooked stock. *Potential consequence:* Increased return rate, costs. *Countermeasure:* Structured data enforced via UCP.

Hypothetical Scenario: Unauthorized Buy Risk

Hypothetical example: An agent buys without a budget check because the identity policy is missing. *Potential liability:* Wallet provider (AP2) or merchant. *Countermeasure:* Thresholds in policies.

Hypothetical Scenario: Fraud Attack Vector

Hypothetical example: Forged credentials enable mass purchases. *Countermeasure:* Verifiable credentials in AP2, anomaly detection.

11.2 Risk-Control Matrix

11.3 Liability Distribution

- **Agent Provider:** Liable for protocol errors
- **Merchant:** Liable for policy gaps and insufficient data
- **Wallet Provider:** Liable for payment errors within AP2
- **User:** Finally responsible for agent authorization

Risk: Uncontrolled Risks

Every incident lowers your Trust Score. Implement proactive controls before agent launch.

Risk	Control	Protocol	Responsible	Monitoring
Hallucination	Structured data; schema validation	UCP/AXP	Catalog	Spot checks
Unauth. Buy	Budget limits, approval	AP2, policy	Trust	Real-time alerts
Identity Fraud	Verifiable credentials	AP2/A2A	Agent Partner-ship	Anomaly detection
Liability Gap	Clear T	Cs, insurance	Legal	Legal
Incident log				
Data Breach	Consent, encryption	MCP/UCP	Trust	Quarterly audit

Table 15: Risk-Control Matrix with detailed controls.

12 Winners and Losers

This chapter analyzes which actors win and which lose in Agentic Commerce—based on concrete mechanisms of value shift, not on speculation.

12.1 Mechanics: Who Owns What?

The value shift depends on four keys. Those who control these win. Those who ignore them lose.

12.1.1 Owning Distribution

Winner: Protocol-capable merchants with UCP integration who keep their product data machine-readable and up to date. *Mechanics:* Agents scan via UCP—best data wins. Merchants with complete, structured data are found and purchased from more frequently.

Loser: SEO-dependent merchants without protocol connectivity. *Mechanics:* Classic search engines are losing relevance. Those who rely only on Google rankings lose agent traffic.

Actionable Recommendation: UCP compliance is not an option but a requirement. Investment in data quality pays off directly in agent reach.

12.1.2 Owning the Wallet: The PayPal Paradigm

Winner: Wallets with AP2 integration (e.g., PayPal, Apple Wallet). *Mechanics:* In the past, the user authenticated every purchase ("Click to Pay"). In 2026, the user authenticates the *agent* once.

PayPal won this shift by opening the **"Identity-for-Agents" infrastructure** (September 2025). They solve the so-called "M x N problem" (M agents interact with N merchants) by giving agents a verifiable, cryptographic identity.

PayPal Agentic Commerce Services:

- **StoreSync:** Product feed integration and cart orchestration
- **Smart Wallet:** Vaulted payment experience without redirects
- **400M+ Active Accounts:** Global reach in 200+ markets
- **25+ Years of Trust:** Fraud prevention, identity verification, buyer-seller protection

Loser: Banks and PSPs that insist on 3D-Secure and manual two-factor checks. These break autonomous agent flows and lead to "cart abandonment by bot."

Actionable Recommendation: Action for Merchants

Activate "Agentic Payments" in your PSP backend. Ensure that your checkout accepts PayPal AP2 tokens—otherwise, you block instant orders from ChatGPT, Microsoft Copilot, and Google Shopping Agent.

12.1.3 Owning Trust

Winner: Aggregators with quality signals via AXP, verified Trust Scores. *Mechanics:* Agents use Trust Scores for decisions. Merchants with high, verified scores are preferred.

Loser: Isolated silos without trust signal integration. *Mechanics:* Agents cannot aggregate isolated reviews. Those who do not provide machine-readable trust signals appear less trustworthy.

Actionable Recommendation: Trust signals must be machine-readable. Returns excellence, incident history, and verification—everything must be communicable via AXP.

12.1.4 Owning the Experience Layer

Winner: AR/3D tools via AXP, embedded experiences. *Mechanics:* Experience platforms significantly increase conversion. Merchants with rich content win against standard providers.

Loser: Static shops without experience components. *Mechanics:* Agents can provide standard product data. Those who do not offer differentiating experiences become standard products.

Actionable Recommendation: Start with an AR pilot in one category. Measure: embedding rate and conversion uplift. Target: 10

12.2 Value Shift: Concrete Numbers (Scenario Hypotheses)

Segment	Winner	Loser	Take Rate Shift	Status
Payments	**Agent Wallets** (AP2)	Legacy Checkout	+0.5–1% new	Hypothesis*
Findability	**Protocol-capable** (UCP)	SEO-dependent	2–5% new	Hypothesis*
Experience	**AR/3D Tools** (AXP)	Static Content	10–20% uplift	Hypothesis*
Data	Signal Aggregators	Review Silos	0.1–0.5% new	Hypothesis*

Table 16: Value shift (Scenario 2030). This table shows which actors profit in which segments—so you can set investment priorities. *Hypothesis = illustrative assumption, not a forecast.

Rationale for Take Rates:

- *Findability:* Agents monetize recommendations (similar to affiliate marketing)
- *Experience:* Conversion uplift justifies premium pricing
- *Payments:* Wallet providers can charge fees for agent transactions

Thesis: Winners 2030

Winners control protocols and experiences. Losers ignore the shift.

Implications by Target Group – Part III

If you are a Merchant:

- UCP compliance is mandatory, AXP experience is the refinement—both are necessary
- Decide build vs. buy based on your core competence (usually: buy for protocols)
- Use PayPal StoreSync as a fast entry point into agent surfaces
- **No-Go:** Do not build proprietary agent APIs—that does not scale

If you are a Platform:

- Protocol reference implementations are strategic (cf. SwagUcp)
- Experience platform as a differentiator for your customers
- Integrate StoreSync and similar services for fast agent connectivity
- **No-Go:** Do not compete against open standards—cooperate

If you are an Investor:

- Protocol stack position in the Mental Model shows strategic relevance
- Wallet position (PayPal, Apple) is high-value—high switching costs
- Experience tech startups profit from the AXP standard
- **No-Go:** Do not underestimate the speed of adoption—productive systems exist today

Epilogue: The Last Merchant – Continued

Five years later. The same morning walk, the same street.

The "last merchant" is still there—but no longer alone. His shop is now an experience hub. Customers come to touch, experience, and for the community. Transactions run via agents—but his Trust Score is the highest, his data the best, and his experiences the most differentiated.

Three doors down, a young merchant has opened. He never did SEO, never ran ads. His entire business runs through agent channels. He calls it "protocol-capable."

The Moral: Commerce is not dying. It is transforming. Winners understand that agents are the most efficient sales channel—if you know how to play the game.

Thesis: Commerce 2030

Commerce 2030 = Human $\times$ AI. The multiplier decides.

The Three Currencies—one last time:

- **Protocols** secure visibility. Without UCP, AXP, and AP2, you do not exist for agents.
- **Trust** secures selection. Agents prefer verified, reliable merchants.
- **Experience** secures margin. Those who only provide data become standard products. Those who offer experiences remain differentiated.

This is the key thesis of this strategy book. Everything else follows from it.

Clarification: Agentic Commerce is not a futuristic tale but an operational reality with clear KPIs, risks, and investment decisions. The introductory phase is already underway (2024–2026), and productive agent checkouts exist today.

Glossary

A2A
Agent2Agent Protocol – communication between agents. Linux Foundation, 21.5k+ GitHub stars.

ACP
Agentic Commerce Protocol – an open, productively used checkout standard for agentic purchase conclusions (Instant Checkout). Licensed under Apache 2.0 and maintained by OpenAI and Stripe. Basis for OpenAI Instant Checkout in ChatGPT.

Agentic Commerce Alliance
Global industry alliance for open standards. Founded July 2025 by Shopware under the leadership of Stefan Hamann. www.agentic-commerce.org

Agent Order
An order initiated by an agent using standardized agent credential headers/tokens (verified agent identity).

Agent Surface
Interface for agent-user interaction (chat, voice, browser).

Agent-assisted
Agent recommends, human decides.

Agent-executed
Agent decides and acts within policies.

Agentic Commerce
Commerce with agents as delegated buyers.

AP2
Agent Payments Protocol – a standard for payment mandates and secure, cryptographically verifiable agent payment authorization. Google/industry standard.

AXP
Agentic Experience Protocol – rich content (3D, AR), quality signals, and experience embedding. Developed by Shopware and the Agentic Commerce Alliance.

Capability Ladder
5-level maturity model for Agentic Commerce readiness.

Cart Orchestration
PayPal service for cart lifecycle management in Agentic Commerce.

Data Fill Rate
Completeness of product data.

Digital Sales Rooms
Shopware feature for video-based consulting—emotional value zone.

Embedding Rate
Percentage of sessions in which experience components are actually rendered.

Experience Embedding
Embedding of rich content (3D, AR, configurators) into agent interfaces via AXP.

Emotional Value Zone
Area with non-automatable added value (sensory experience, identity, community, serendipity, expertise).

Human-in-the-Loop
Human confirmation in processes.

Identity-for-Agents
PayPal infrastructure for agent identification, solving the M x N problem.

M x N Problem
Challenge: M agents must communicate authentically with N merchants. Solved by central identity providers (PayPal, Visa TAP).

MCP
Model Context Protocol – basic context transport. Anthropic, November 2024. Common integration layer supported by Anthropic, OpenAI, and Google.

Merchant of Record
Legally responsible party for a transaction.

Policy Abort Rate
Rate of abortions due to policy violation.

Policy File
Machine-readable rules at `/.well-known/agent-policy.json`.

Protocol-capable
Merchants with native UCP/AXP/AP2 integration that are directly reachable by agents via standardized protocols.

Quality Signals
Structured trust indicators (reviews, returns, merchant trust) via AXP.

RACI
Responsibility Matrix (Responsible, Accountable, Consulted, Informed).

Smart Wallet
Digital wallet with agent authorization (e.g., PayPal Smart Wallet).

Spatial Commerce
Shopware feature for 3D/AR product experiences (Apple Vision Pro, Meta Quest).

StoreSync
PayPal service for product feed integration and cart orchestration in Agentic Commerce.

Trust Score
Internal KPI construct from quality signals. External agents use similar signals with their own weighting.

UCP
Universal Commerce Protocol – end-to-end commerce protocol for discovery, capability description, order, and checkout orchestration. Google Initial Release January 2026, endorsed by 20+ companies.

Update Speed
Sync latency between backend and agent (median of sync time).

Verifiable Credentials
Cryptographically verifiable proofs (AP2, Visa TAP).

Visa TAP
Visa Trusted Agent Protocol – agent identity, consumer recognition, and payment information (Visa, October 2025).

Further Resources

This strategy book is part of a comprehensive ecosystem of resources on the topic of Agentic Commerce.

Protocol Portals

Further Protocol Documentation:

- **UCP (Google):** https://developers.google.com/merchant/ucp
- **AP2 (Google):** https://developers.google.com/payments/ap2

Agentic Commerce Alliance

Website: https://www.agentic-commerce.org

The global industry alliance for open standards. Founded by Shopware under the leadership of Stefan Hamann. Membership, working groups, protocol governance, and industry events.

Expert Blog & Research

Website: https://www.agentic-commerce.sh

Stefan Hamann's personal platform with strategic analyses, deep dives, and current developments:

- **Whitepapers:** Technical and strategic guides for download
- **Industry Reports:** Analyses of McKinsey, Morgan Stanley, IBM/NRF
- **Protocol Updates:** Latest developments in UCP, AXP, AP2

Technical Whitepapers

Agentic Commerce – Protocols, Standards, and Reference Architectures
Developer Technical Guide, January 2026, 60 min read

Comprehensive technical guide: UCP, AXP, A2A, ACP, and AP2 protocols, implementation strategies, and API examples.

Industry Reports (Primary Sources)

Source	Report	Key Insight
McKinsey	The Agentic Commerce Opportunity	Six-Domain Business Model Framework
Morgan Stanley	Market Outlook 2030	$190–385B US spending by 2030
IBM + NRF	Own the Agentic Experience	Consumer spending trends
Google Cloud	Retail Readiness Guide	Implementation best practices
PayPal Ventures	State of Agentic Commerce	Identity-for-Agents infrastructure

Table 17: Industry Reports: Primary sources for strategic analysis.

Protocol Repositories (Open Source)

- **UCP:** https://github.com/Universal-Commerce-Protocol/ucp (Apache 2.0)
- **AXP:** https://github.com/agentic-commerce-lab/AXP-protocol (Shopware/Alliance)
- **ACP:** https://github.com/agentic-commerce-protocol/agentic-commerce-protocol (OpenAI/Stripe)
- **A2A:** https://github.com/a2aproject/A2A (Linux Foundation)
- **SwagUcp:** https://github.com/agentic-commerce-lab/SwagUcp (Shopware reference implementation)

PayPal Agentic Commerce

Documentation: https://developer.paypal.com/docs/agentic-commerce/

Services: StoreSync (Product Feed + Cart Orchestration), Smart Wallet, Identity-for-Agents

Partnerships: OpenAI (ChatGPT), Microsoft (Copilot), Perplexity, Google Cloud, Shopware