AGENTIC COMMERCE

Wie der Handel 2030 überlebt

STRATEGIEBUCH

Agenten revolutionieren den Handel. Dieses Strategiebuch analysiert die Mechanik dieser Disruption und zeigt dir als Händler, Plattform-Betreiber, Tech-Entscheider oder Investor konkrete Strategien für die Ära des Agentic Commerce.

AUTOR

Stefan Hamann

VERSION

v1.3 – Januar 2026

Inhaltsverzeichnis

Einführung

Definition: Agentic Commerce

Agenten kaufen im Auftrag von Menschen. Sie treffen Kaufentscheidungen, führen Transaktionen durch und managen After-Sales – mit Erlaubnis des Nutzers, innerhalb definierter Regeln und Budgets.

Was „autonom“ wirklich bedeutet:

Nicht „selbstständig ohne Kontrolle“, sondern „delegiert mit Limits und Audit Trail“.

Zwei Modi:

- **Agent-assisted:** Agent empfiehlt, Mensch entscheidet
- **Agent-executed:** Agent entscheidet und handelt innerhalb Policies

Der Übergang zwischen beiden Modi ist fließend – und genau dort liegt die strategische Chance.

Terminologie in diesem Strategiebuch:

Dieses Dokument verwendet stabile Begriffe und definiert sie im Glossar.

- **Agent** – KI-System, das im Auftrag von Menschen handelt
- **Trust Score** – Internes KPI-Konstrukt, das beobachtbare Signale bündelt
- **Protokollfähig** – Gestufte Integration: Findable (UCP/Feed), Buyable (AP2/ACP), Trust-ready (TAP), Experience-ready (AXP)
- **Emotionale Wertzone** – Bereich mit nicht-automatisierbarem Mehrwert

These: Leitthese

Marktmacht entsteht nicht mehr durch Sichtbarkeit, sondern durch Maschinenlesbarkeit.

Das ist die zentrale Erkenntnis. Alles andere folgt daraus.

Die drei neuen Währungen:

1. **Protokollfähig** – Wer via UCP, AXP und AP2 erreichbar ist, wird gefunden
2. **Trust Score** – Wer verifizierte Quality Signals liefert, wird bevorzugt
3. **Emotionale Wertzonen** – Wer unautomatisierbare Erlebnisse bietet, differenziert sich

Jeder Abschnitt dieses Strategiebuchs wird an dieser These gemessen. Die Frage ist immer: *Wie beeinflusst das meine Position bei Protokollen, Trust oder Experience?*

Prolog: Der letzte Händler

Ein fiktiver Morgenspaziergang durch eine Einkaufsstraße im Jahr 2030: Fast alle Geschäfte sind verschwunden. Käufe wickeln Agenten unsichtbar im Hintergrund ab. Nur ein Laden hat geöffnet – „Der letzte Händler“.

Diese Eröffnungsszene skizziert die Leitfrage dieses Strategiebuchs: **Was bleibt, wenn Agenten einen Großteil der Customer Journey übernehmen?**

Dieses Strategiebuch argumentiert, dass der Handel sich fundamental transformieren wird – aber nicht verschwinden. Die Gewinner werden jene sein, die verstehen: (1) Welche Teile der Wertschöpfung an Agenten fallen, (2) Welche Teile durch menschliche Stärken verteidigt werden können, (3) Wie die neue Architektur aus Protokollen und Trust aussieht, (4) Was das Operating Model eines agentenfähigen Händlers ausmacht.

Zielgruppen

Händler: Playbook für die Transformation – Datenstrategie, Trust-Signale, Operating Model.

Tech-Entscheider: Architekturentscheidungen, Eigenentwicklung vs. Partner, Protokolllandschaft.

Investoren: Wertverschiebung in der Architektur, Moats, Gewinner-Verlierer-Hypothesen.

Methodik und Quellen

Die Analysen basieren auf öffentlich verfügbaren Ankündigungen, Protokollspezifikationen und Szenarioanalysen. Wo konkrete Zahlen genannt werden, sind diese als *Szenarien* zu verstehen, nicht als deterministische Prognosen. Primärquellen sind im Text verlinkt.

Das Agentic Commerce Mental Model

Dieses Diagramm ist die eine Grafik, die alles erklärt. Es wird in jedem Teil referenziert und bildet die Grundlage für alle strategischen Entscheidungen.

Der Experience Layer bedient drei Zielgruppen:

- **Agent Experience:** Maschinenlesbare Signale via AXP (Quality Signals, strukturierte Produktdaten, Trust-Indikatoren). Agenten *lesen* Experience als Entscheidungsgrundlage.
- **Human Experience:** Immersive Interfaces (3D, AR, Konfiguratoren, Video-Beratung). Menschen *erleben* Experience emotional und sensorisch.
- **Hybrid Experience:** Agent-assisted Szenarien, in denen Agenten vorfiltern und Menschen final entscheiden. Beide Modalitäten wirken zusammen.

Implikation: Experience ist kein Marketing-Feature, sondern ein struktureller Hebel im Agent Funnel. Wer Experience nur für Menschen baut, verliert Agent-Traffic. Wer Experience nur für Agenten baut, verliert Marge.

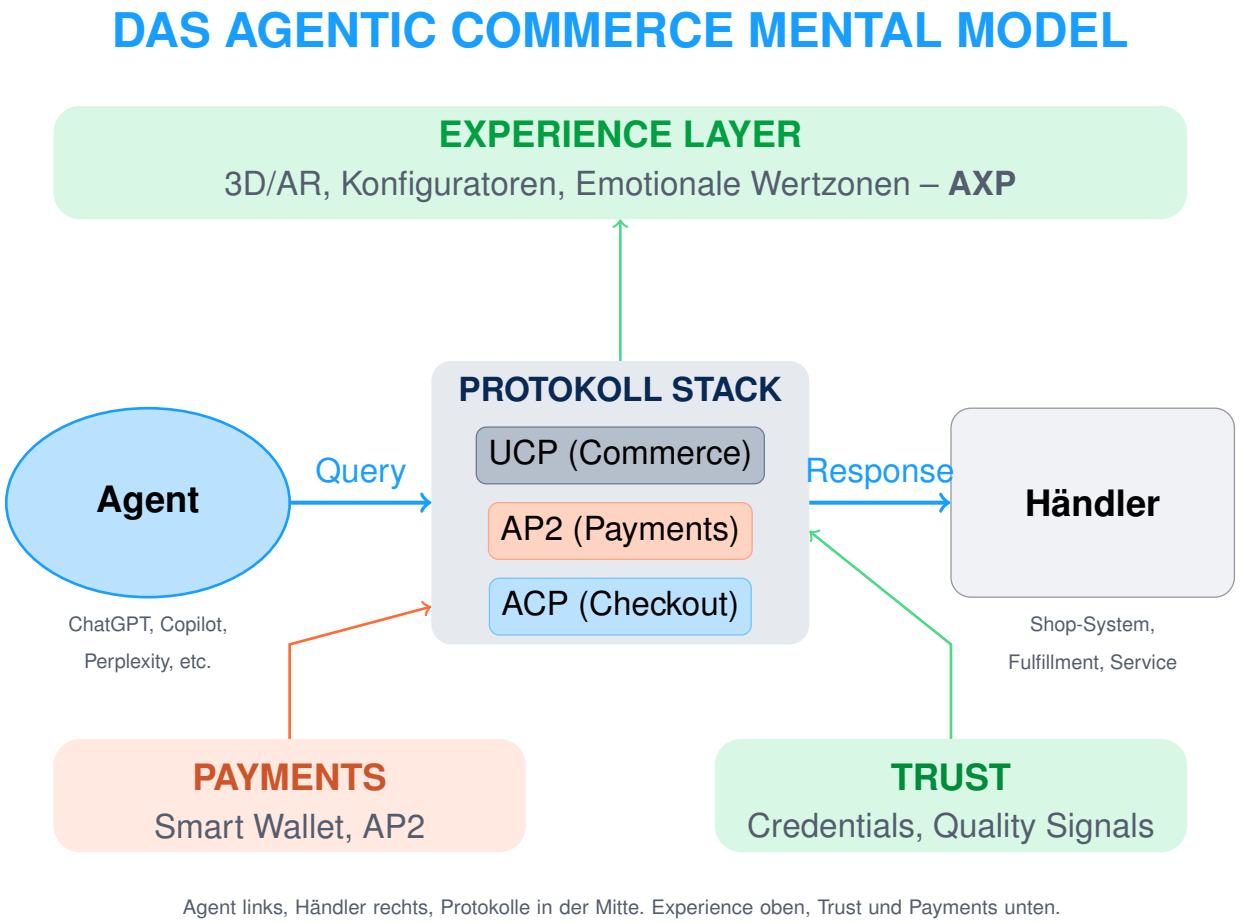

Abbildung 1: Das Agentic Commerce Mental Model: Agent (links) kommuniziert über den Protokoll-Stack (Mitte) mit dem Händler (rechts). Experience Layer (oben) differenziert, Trust und Payments (unten) sichern ab. **Referenz für alle Teile.**

Ressourcen und Ökosystem

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

Das Portal für AXP (Agentic Experience Protocol) und Alliance-Inhalte. Bietet:

- AXP-Dokumentation und Referenz-Implementierungen
- Playground zum Testen von Experience-Flows
- Strategische Whitepapers und Research

Weitere Protokoll-Portale:

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

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

Die globale Industrie-Allianz für offene Standards im Agentic Commerce. Gegründet im Juli 2025 von Shopware unter Führung von Stefan Hamann. Die Alliance vereint Händler, Technologie-Anbieter, Payment-Provider und KI-Unternehmen mit dem Ziel, offene Protokolle zu entwickeln und Monopolstrukturen zu verhindern.

- **Mission:** Human Value Preservation in einer automatisierten Welt

- **Fokus:** Offene Standards, Interoperabilität, Händler-Souveränität
- **Mitglieder:** Führende Retailer, Payment-Provider, Tech-Unternehmen

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

Stefan Hamanns persönliche Plattform mit strategischen Analysen, Deep-Dives und aktuellen Entwicklungen im Agentic Commerce:

- **Whitepapers:** Technische und strategische Leitfäden
- **Protokoll-Updates:** Neueste Entwicklungen in UCP, AXP, AP2
- **Industry Reports:** Analysen zu McKinsey, Morgan Stanley, IBM/NRF

Commerce-Protokolle (Details in Teil III):

- **UCP:** Universal Commerce Protocol – End-to-End-Orchestrierung
- **AXP:** Agentic Experience Protocol – Rich Content & Quality Signals
- **AP2:** Agent Payments Protocol – Sichere Zahlungsmandate
- **A2A:** Agent2Agent Protocol – Multi-Agent-Koordination
- **ACP:** Agentic Commerce Protocol – Instant Checkout (OpenAI/Stripe)
- **StoreSync:** PayPal's Katalog- und Cart-Orchestrierung

TEIL I

Strategische Einordnung

1 Das Zeitalter der Agenten

Wenn du dieses Kapitel überspringst: Du optimierst weiter auf SEO und Ads, während Agenten bereits über Protokolle kaufen. Das ist kein Detailfehler – das ist strategischer Blindflug.

1.1 Die Mechanik der Disruption

1.1.1 Warum Distribution kippt

Die fundamentale Disruption liegt in der **Verschiebung der Gatekeeper-Position**. Bisher kontrollierten drei Akteure den Zugang zum Kunden:

Heutige Distribution: Ein signifikanter Anteil des E-Commerce-Traffics beginnt in Suchmaschinen (Szenario: 30–50%, variiert je Kategorie und Region), Marktplätzen und Social Platforms. Diese Gatekeeper aggregieren die Auffindbarkeit und leiten Traffic weiter.

Warum Agents das ändern: Agenten kennen den Bedarf, bevor der Nutzer explizit sucht. Sie vergleichen über Plattformgrenzen hinweg und kuratieren basierend auf persistenten Nutzerpräferenzen. Agenten organisieren die Auffindbarkeit anders: nicht über zentrale Portale, sondern durch direkte Protokoll-Anfragen an Händler-APIs.

Folge: Gatekeeper transformieren sich von Traffic-Aggregatoren zu Protokoll-, Wallet- oder Trust-Layern. Händler mit direkter Protokoll-Anbindung gewinnen – unabhängig von bisheriger SEO-Position oder Marktplatz-Präsenz.

Schlüsselbegriffe (werden im Glossar detailliert):

- **Protokollfähig** – Gestuft: *Findable* (UCP oder Feed + StoreSync), *Buyable* (AP2 oder ACP), *Trust-ready* (TAP oder vergleichbare Credentials), *Experience-ready* (AXP oder ähnliche Experience Signals)
- **Trust Score** – Internes KPI-Konstrukt aus Quality Signals. Externe Agenten nutzen ähnliche Signale, aber mit eigener Gewichtung
- **Agent Order** – Order initiiert durch Agent mittels verifizierter Agent-Identity
- **Emotionale Wertzone** – Bereich mit nicht-automatisierbarem Mehrwert (Sensorik, Identität, Community)

1.1.2 Der neue Funnel – mit Merchant Levers

Glossar der Messgrößen:

- **API Reichweite:** Anteil der Agenten, die dein Sortiment technisch erreichen können (Feeds plus

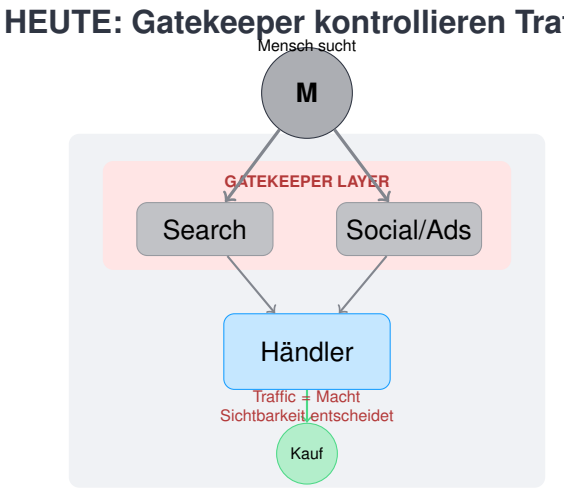

Abbildung 2: Heute: Gatekeeper (Search, Social, Ads) kontrollieren den Zugang zum Kunden. Händler zahlen für Sichtbarkeit.

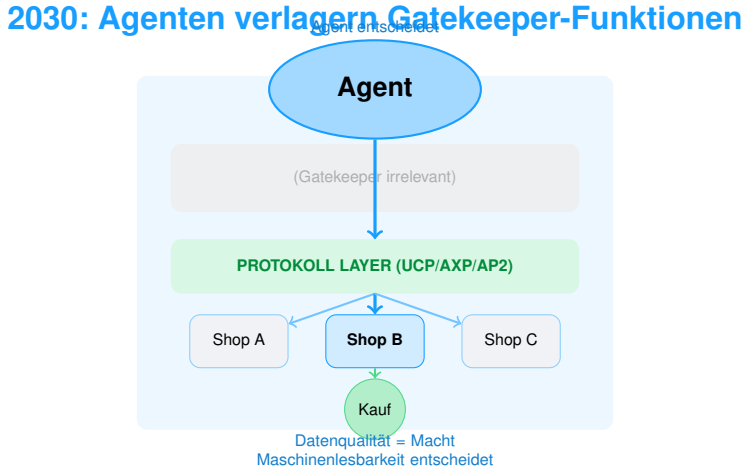

Abbildung 3: Szenario 2030: Agenten umgehen Gatekeeper durch direkte Protokollkopplung. Beste Daten gewinnen, nicht beste Ads.

Phase	Klassisch → Agent	Dein Hebel	Messgröße
Awareness	Ads → Protokoll-Auffindbarkeit	**UCP-Compliance**	API Reichweite
Interest	Website → Präferenzmatrix	Quality Signals	Trust Score
Desire	Produktseite → AXP Data	**Erlebnisinhalt**	Einbettungsquote
Action	Checkout → API-Transaktion	Response Time	Latency P95
Loyalty	Newsletter → Preference Learning	Return Excellence	NPS

Tabelle 1: Funnel-Transformation: Diese Tabelle zeigt, wie sich jede Phase verändert – damit du die richtigen Hebel priorisierst.

APIs plus Verfügbarkeit).

- **Trust Score:** Internes KPI-Konstrukt aus Verifikation, Returns, Incident Historie. Externe Agenten nutzen ähnliche Signale mit eigener Gewichtung.
- **Einbettungsquote:** Anteil Sessions, in denen deine Experience-Komponente tatsächlich gerendert wird.
- **Latency P95:** 95. Perzentil der Response-Zeit für Agent-Anfragen. Kritisch, da Agenten harte Timeouts haben.

Was du daraus ableitest:

- **API Reichweite unter 80%?** Dann können mehr als 20% der Agenten dein Sortiment nicht finden – du bist für einen großen Teil des Agent-Traffics schlicht unsichtbar.
- **Trust Score schlägt Conversion Rate:** Agenten bewerten dich nicht nach klassischen Conversion-Metriken, sondern nach deinem Trust Score. Ein niedriger Score führt zu niedrigerer Priorisierung.
- **Latency P95 ist conversion-kritisch:** Agenten haben harte Timeouts (typisch: wenige Sekunden). Zu langsame APIs führen zu Abbrüchen – Latency ist kein reines Tech-Detail, sondern ein direkter Umsatzfaktor.

1.1.3 Wertflüsse im neuen Modell

Drei Flüsse im Agentic Commerce: Daten, Trust und Geld fließen über unterschiedliche Kanäle. Die folgenden drei Diagramme zeigen jeden Fluss separat – mit identischen Akteuren in gleicher Position für einfachen Vergleich.

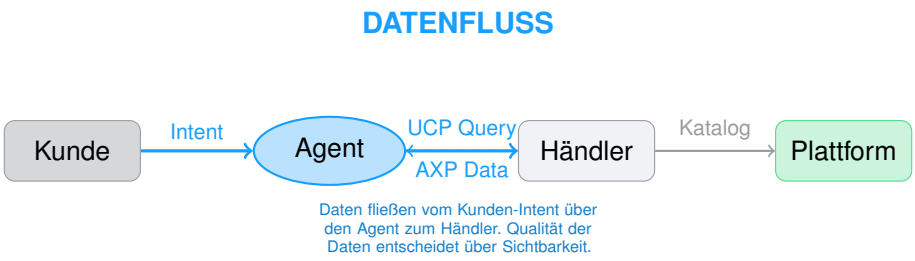

Abbildung 4: Datenfluss: Intent → Agent → UCP Query → Händler. Rückkanal: AXP-Produktdaten.

Abbildung 5: Trustfluss: Consumer Recognition → Agent Credentials → Händler. Mandates an Wallet.

Risiko: Transformation der Gatekeeper

Folgende Akteure müssen ihre Rolle transformieren oder verlieren Gatekeeper-Position: SEO/SEA-Agenturen, Affiliate-Netzwerke, Preisvergleichsportale, klassische Review-

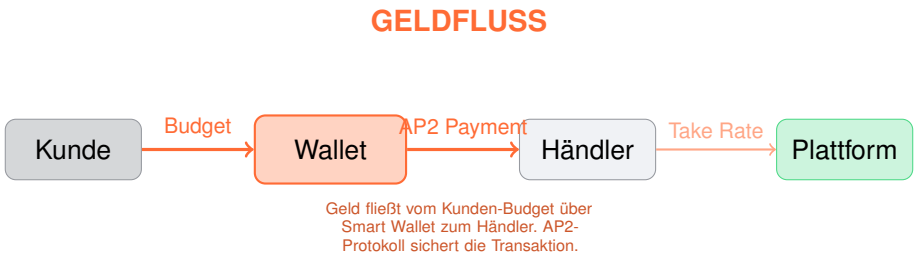

Abbildung 6: Geldfluss: Budget → Smart Wallet → AP2 Payment → Händler. Take Rate an Plattform.

Plattformen, Retargeting-Anbieter. Erfolgreiche transformieren sich zu Protokoll-, Wallet- oder Trust-Layern.

1.2 Evidenz: Meilensteine 2024–2026

Die folgende Timeline dokumentiert die technischen Durchbrüche und Markt-Meilensteine, die den Agentic Commerce von einer Vision zur operativen Realität gemacht haben.

Zeitpunkt	Entwicklung und Primärquelle	Status
25.11.2024	**Anthropic MCP:** Standardisiert LLM-Datenzugriff und Tool-Integration.[1]	Produktiv
23.01.2025	**OpenAI Operator:** Erster Agent für Browser-Steuerung und Käufe.[2]	Pilot
16.09.2025	**Google AP2:** Agent Payments Protocol mit Mandates und Verifiable Credentials.[3]	Initial Release
29.09.2025	**OpenAI Instant Checkout + ACP:** ChatGPT erhält Checkout auf Basis von ACP.[4]	Produktiv
14.10.2025	**Visa TAP:** Trusted Agent Protocol für Agent Identity und Fraud-Prävention.[5]	Verfügbar
28.10.2025	**PayPal Agentic Commerce:** Launch von Agentic Commerce Services.[6]	Rollout
25.11.2025	**PayPal + Perplexity:** Instant Buy Integration mit StoreSync.[7]	Rollout
08.01.2026	**Microsoft Brand Agents:** Copilot Checkout, referenziert ACP als Standard.[8]	Produktiv
11.01.2026	**Google UCP 1.0:** Universal Commerce Protocol, endorsed by 20+ Partner.[9]	Initial Release

Tabelle 2: Timeline: Der Weg zum Agentic Commerce (2024–2026). **Produktiv** = Live im Markt, **Initial Release** = Veröffentlichte Spezifikation, **Pilot** = Testphase.

Definition: MCP als Integrationsschicht

Das Model Context Protocol (MCP), angekündigt von Anthropic am 25. November 2024, ist die gemeinsame Integrationsschicht, die von mehreren Agent-Plattformen unterstützt wird (Anthropic, OpenAI, Google). **Vor MCP** musstest du eine eigene API für jeden KI-Bot bauen. **Mit MCP** exponierst du einen standardisierten „Resource Server“, den Claude, ChatGPT, Gemini und andere LLMs gleichermaßen lesen können. UCP, ACP und AP2 unterstützen MCP oder sind kompatibel damit – sie bauen darauf auf, sind aber eigenständige Commerce-Protokolle.

Hypothetisches Szenario: Perplexity Shopping Integration

Die Perplexity Shopping-Integration entwickelte sich in drei Stufen:

- **Juli 2025:** Comet Browser erste Verfügbarkeit (Early Access)
- **Oktober 2025:** Breiterer Launch mit Shopping-Funktion
- **25. November 2025:** PayPal Instant Buy Integration angekündigt

Agent übernimmt Produktauswahl, Händlervergleich, Checkout. *Status: Rollout-Phase, keine öffentlich kommunizierten Volumina.*

1.3 Marktpotenzial: Die Zahlen hinter dem Hype

Die strategische Relevanz von Agentic Commerce wird durch unabhängige Analysen führender Beratungshäuser und Finanzinstitute untermauert:

Kategorie	Quelle	Prognose	Status
Spending Shift	Morgan Stanley[10]	**$190–385 Mrd.** US-E-Commerce-Ausgaben durch agentische Käufer bis 2030	Szenario*
Orchestrated Revenue	McKinsey[11]	„Seismic shift“ – Agenten führen Multi-Step Commerce Flows aus	Analyse
Survey Insights	IBM + NRF[12]	Fundamentale Veränderung des Consumer Spendings erwartet	Erhebung
Tech Readiness	Google Cloud	Retail Readiness als kritischer Wettbewerbsfaktor	Produktiv

Tabelle 3: Marktprognosen nach Kategorie: *Spending Shift* = Umsatzverlagerung, *Orchestrated Revenue* = Agent-gesteuerte Flows, *Survey Insights* = Konsumentenbefragung, *Tech Readiness* = Infrastruktur. *Szenario-Werte sind Schätzungen, keine Prognosen.

Strategische Implikation (McKinsey): Agentic Commerce ist „nicht nur ein Trend, sondern ein struktureller Sprung“. Traditioneller E-Commerce optimiert auf Clicks, Conversions und kreative Kampagnen. Agentic Commerce verlagert *Entscheidungsrechte* von Menschen auf intelligente autonome Agenten.

These: Disruption der Distribution

Die eigentliche Disruption ist der Verlust der Gatekeeper-Position. Händler mit direkter Protokoll-Anbindung gewinnen – unabhängig von bisheriger SEO-Position.

Handlungsempfehlung: Was du jetzt anders machst

Diese Woche:

- Budget-Split analysieren: SEO/SEA vs. Datenqualität/API-Readiness
- **Erstes Artefakt:** Eine Seite mit aktuellem Split und Ziel-Split

Nächste 14 Tage:

- KPI „Agent Orders“ und „API Reichweite“ im Dashboard einführen
- **Verantwortung:** Head of E-Commerce oder CTO

Nächste 30 Tage:

- Agent-Channel-Verantwortlichen benennen (nicht IT, nicht Marketing allein)

2 Customer Journey 2030

Wenn du dieses Kapitel überspringst: Du optimierst weiter auf Website-Besuche und Produktseiten-Views, während die echte Conversion längst in API-Responses und Trust Scores entschieden wird.

Die Customer Journey verändert sich fundamental, wenn Agenten als Intermediäre auftreten. Klassische Funnels (AIDA: Awareness, Interest, Desire, Action) bleiben als Konzept bestehen – aber die *Akteure* und *Touchpoints* verschieben sich. Statt Menschen, die Websites besuchen, interagieren Agenten mit APIs. Statt emotionaler Werbebotschaften entscheiden strukturierte Daten und Trust Scores.

Dieses Kapitel zeigt dir Phase für Phase, welche Risiken entstehen und wie du ihnen begegnest. Die Tabelle fasst die wichtigsten Fehlermuster zusammen und ordnet jedem die passende Gegenmaßnahme und das relevante Protokoll zu.

2.1 Phase-für-Phase mit Gegenmaßnahmen

Phase	Risiko (Fehlermuster)	Deine Gegenmaßnahme	Protokoll
Bedarf	False Positives	Confidence Thresholds	MCP
Recherche	Incomplete Data	**Schema Validation**	UCP
Auswahl	Halluzination	**Structured Data only**	AXP
Checkout	Payment Reject	Retry + Fallback	ACP/AP2
After-Sales	Sync-Fehler	Event Sourcing	Webhooks

Tabelle 4: Journey-Phasen mit Risiken: Diese Tabelle zeigt, was schiefgehen kann und wie du es verhinderst.

Was du daraus ableitest:

- Halluzination ist kein LLM-Problem – es ist ein Datenqualitäts-Problem. Deine Gegenmaßnahme: Structured Data.
- Payment Reject ist der teuerste Fehler. Retry + Fallback muss automatisiert sein.
- After-Sales-Sync-Fehler zerstören Trust Score. Event Sourcing ist keine Option, sondern Pflicht.

Abbildung 7: Strategiematrix: Wo Agenten gewinnen (rechts) und wo Menschen differenzieren (oben). **INVESTIEREN** = Ressourcen aufbauen. **VERTEIDIGEN** = Margen schützen. **SPEZIALISIEREN** = Nische finden.

2.2 Automatisierbarkeit vs. Differenzierung

Definition: Experience im Agentic Commerce

Experience ist kein Feature, sondern ein systemisches Operating System für Entscheidungen und Vertrauen:

Experience = Entscheidungsfähigkeit + Vertrauen + Emotion

- **Entscheidungsfähigkeit:** Reduktion von Komplexität durch strukturierte Präsentation von Optionen, Vergleichen und Konsequenzen
- **Vertrauen:** Inszenierung von Quality Signals, Reviews, Zertifikaten und Händler-Reputation als erlebbare Sicherheit
- **Emotion:** Sensorische und identitätsstiftende Erlebnisse, die Agenten nicht replizieren können

Wichtig: AR, VR und 3D sind Ausgabekanäle für Experience, nicht Experience selbst. Experience wirkt auf drei Ebenen: für Agenten (maschinenlesbare Signale via AXP), für Menschen (immersive Interfaces) und für hybride Szenarien (Agent-assisted Shopping).

2.3 Emotionale Wertzonen

Bereiche, in denen menschliche Erfahrung Differenzierung ermöglicht:

1. **Sensorische Erlebnisse:** Touch, Smell, Fit – nicht digitalisierbar. Agenten können Produktbeschreibungen liefern, aber das haptische Erlebnis, der Geruch von Leder oder die Passform einer Jeans bleiben menschliche Domäne. Händler, die Showrooms, Fitting-Rooms oder Sample-Programme anbieten, schaffen unkopierbare Differenzierung. *Wichtig:* AR und VR sind Verstärker dieser Erlebnisse, nicht die Differenzierung selbst – sie reduzieren

Unsicherheit, ersetzen aber nicht das physische Erleben.

2. **Identitätsstiftende Käufe:** Luxus, Geschenke, Custom-Produkte – das „Warum“ zählt mehr als das „Was“. Agenten optimieren auf Effizienz und Preis, aber emotionale Käufe (Geschenke, Erinnerungsstücke, Statussymbole) brauchen menschliche Beratung und Storytelling. Händler, die die persönliche Bedeutung von Käufen verstehen und kommunizieren, gewinnen.
3. **Community:** Fans, Sammler, Zugehörigkeit – nicht von Agenten erzeugbar. Communities entstehen durch gemeinsame Leidenschaft, Events, Exklusivität. Agenten können Empfehlungen geben, aber keine echte Zugehörigkeit schaffen. Händler mit aktiven Communities (Sammler-Clubs, VIP-Programme, Events) bauen nachhaltige Moats.
4. **Serendipität:** Überraschung, Entdeckung – Agenten optimieren auf Bekanntes. Algorithmen zeigen, was ähnlich ist. Menschen entdecken durch Zufall, durch Stöbern, durch persönliche Empfehlungen. Händler, die Kuratierung, Personal Styling oder unerwartete Kombinationen anbieten, schaffen Mehrwert, den Agenten nicht replizieren können.
5. **Expertise und Beratung:** Komplexe Produkte brauchen menschliche Expertise. Technische Beratung, medizinische Geräte, B2B-Lösungen – hier zählt Vertrauen in menschliche Kompetenz. Agenten können Daten liefern, aber keine echte Beratungsbeziehung aufbauen.

Strategische Implikation: Emotionale Wertzonen sind keine Nische – sie sind die Differenzierung in einem automatisierten Markt. Händler sollten systematisch identifizieren: Welche Teile meines Geschäfts können Agenten nicht replizieren? Diese Bereiche ausbauen, nicht reduzieren.

These: Emotionale Wertzonen

Die Automatisierung macht menschliche Stärken wertvoller. Händler, die ihre emotionalen Wertzonen identifizieren und ausbauen, bleiben differenziert. Agenten übernehmen Standardkäufe – das macht menschliche Erlebnisse wertvoller, nicht überflüssig.

Fallbeispiel: Best Practice: Shopware Spatial Commerce & Digital Sales Rooms

Während Agenten die Transaktion („Buying“) übernehmen, muss der Händler das Erlebnis („Shopping“) neu definieren. Shopware hat mit **Spatial Commerce** und **Digital Sales Rooms** Werkzeuge geschaffen, die Agenten nicht replizieren können:

- **Human Connection:** Video-gestützte Beratung im Digital Sales Room schafft Vertrauen bei High-Value-Produkten. Ein Agent kann Daten liefern, aber keine echte menschliche Verbindung aufbauen.
- **3D/Spatial:** Produkte werden in 3D erlebbar (Apple Vision Pro, Meta Quest). Diese Daten werden via AXP (Agentic Experience Protocol) zwar referenziert, aber nur im Shop tatsächlich *erlebt*.
- **Configurator Experiences:** Komplexe Produkt-Konfiguratoren (Möbel, Fahrzeuge, Mode) bieten interaktive Erlebnisse, die über reine Datenabfragen hinausgehen.

Takeaway: Nutzen Sie Agenten für die Logistik des Kaufs, aber Shopware-Features für die Emotion der Entscheidung. Die Kombination ist der Wettbewerbsvorteil.

Handlungsempfehlung: Was du jetzt anders machst

Diese Woche:

- Customer Journey Map um Agent-Touchpoints erweitern
- **Erstes Artefakt:** Neue Journey Map mit 5 Agent-Phasen

Nächste 14 Tage:

- Human Value Audit: Deine 3 stärksten nicht-automatisierbaren Erlebnisse identifizieren
- **Verantwortung:** Product + Marketing gemeinsam

Nächste 30 Tage:

- AR/3D-Pilot in einer Kategorie mit hohem Sensorik-Bedarf starten

Implikationen nach Zielgruppe – Teil I

Wenn du Händler bist:

- Die Disruption betrifft deine Distribution – nicht dein Produkt
- Investiere in Datenqualität (UCP), nicht in mehr Ads
- Identifiziere deine Human Value Islands als Differenzierung
- **No-Go:** Ignoriere nicht die Agent-Channel-Readiness – das ist existenziell

Wenn du Plattform bist:

- Deine Gatekeeper-Position transformiert sich zu Protokoll- oder Trust-Layer
- Offene Standards (UCP, AXP) sind strategisch wichtiger als proprietäre APIs
- Positioniere dich als Enabler, nicht als Bottleneck
- **No-Go:** Blockiere nicht Agent-Zugriff – das beschleunigt Disintermediation

Wenn du Investor bist:

- Die Wertverschiebung geht von Traffic zu Protokollen und Trust
- Protokollfähige Händler sind besser positioniert als SEO-abhängige
- Experience-Tech (AR/3D/AXP) ist Differenzierungshebel, nicht Nice-to-have
- **No-Go:** Bewerte Unternehmen nicht nach alten E-Commerce-KPIs – Agent Adoption ist relevanter

TEIL II

Operative Ableitung

3 Operating Model 2030

Wenn du dieses Kapitel überspringst: Du startest Agent-Integrationen ohne klare Ownership. Das Ergebnis: Finger-Pointing zwischen IT, Marketing und Operations. Und am Ende scheitert die Integration an internen Silos, nicht an Technik.

3.1 Neue Rollen und Systeme

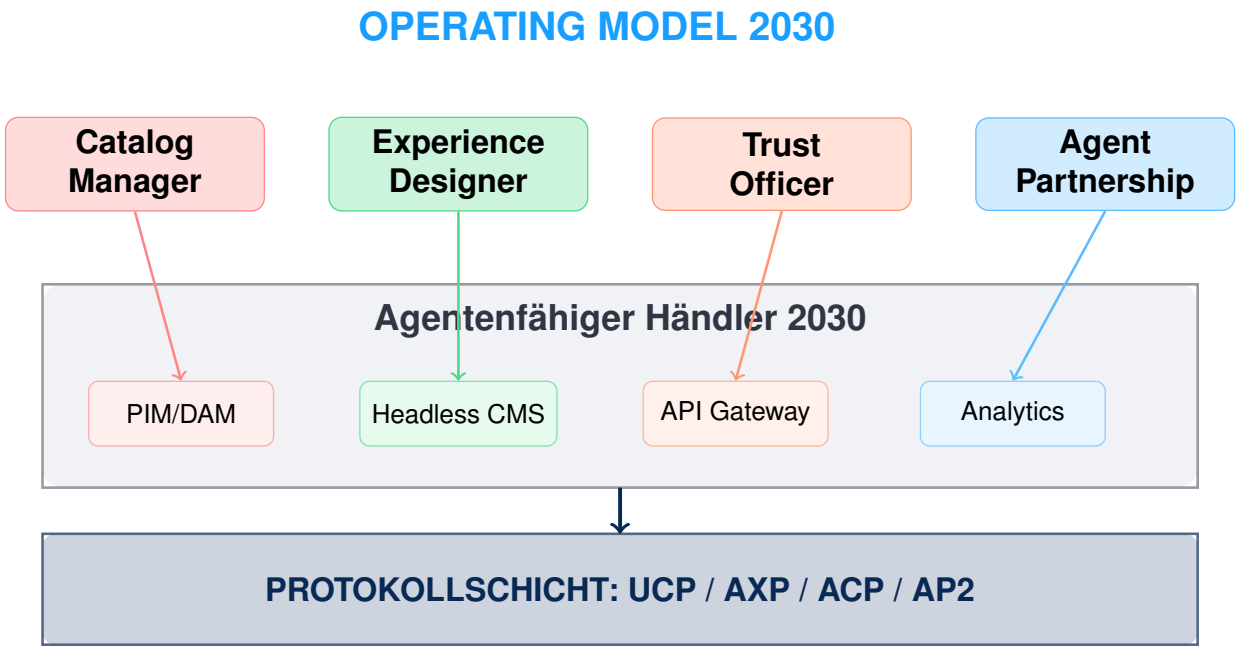

Abbildung 8: Operating Model 2030: Vier Kernrollen (oben) steuern spezialisierte Systeme (Mitte), die über die gemeinsame Protokollschicht (unten) mit Agenten kommunizieren.

Experience-Rolle: Kernaufgaben

Die Experience-Rolle ist *nicht* Content-Management, sondern Decision Design. Die Aufgaben:

- **Entscheidungsreduktion:** Gestaltung von Vergleichen, Filtern und Empfehlungslogiken, die Komplexität für Nutzer und Agenten reduzieren
- **Trust-Inszenierung:** Präsentation von Quality Signals, Reviews und Zertifikaten als erlebbare Sicherheit (nicht als Datenpunkte)
- **Human Handovers:** Definition von Schwellen und Triggern, wann Agenten an Menschen eskalieren (z. B. bei Hochwertkäufen, Customization, Beratungsbedarf)
- **Experience Embedding:** Technische Integration von 3D, AR, Konfiguratoren via AXP in Agent-Surfaces – mit klaren Sandbox-Boundaries

Abgrenzung: Experience ist *nicht* Marketing (Brand Campaigns), *nicht* IT (API-Infrastruktur), *nicht* Support (After-Sales). Experience designt den Moment der Entscheidung.

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**

Tabelle 5: RACI-Matrix: R=Responsible, A=Accountable, C=Consulted, I=Informed. Diese Matrix zeigt Verantwortlichkeiten – damit du Ownership-Lücken identifizierst.

3.3 KPIs pro Rolle (Detail)

Rolle	Top-3 KPIs	Zielwert	Frequenz
Catalog	Data Fill Rate, Update Speed, Schema Compliance	**>95%**, <5 Min, 100%	Täglich
Experience	Decision Completion Rate, Assisted Conversion Rate, Human Handover Rate, Einbettungsquote	>85%, >15%, <8%, >10%	Wöchentlich
Trust	Trust Score, Policy Abort Rate, Incident Resolution	**>75**, <5%, <4h	Täglich
Agent Partnership	Agent Adoption, Conversion Rate, New Integrations	>20%, **>3%**, 2+/Q	Wöchentlich

Tabelle 6: KPIs pro Rolle. Diese Tabelle zeigt, was jede Rolle messen muss – damit du Performance-Probleme früh erkennst.

Neue Experience-KPIs erklärt:

- **Decision Completion Rate:** Anteil der Sessions, in denen Nutzer/Agenten eine Kaufentscheidung treffen (nicht abbrechen). Misst Entscheidungsreduktion.
- **Assisted Conversion Rate:** Anteil der Conversions, bei denen Agent-Experience-Komponenten (Vergleiche, Trust-Signale) genutzt wurden. Misst Experience-Wirkung.
- **Human Handover Rate:** Anteil der Agent-Sessions, die an Menschen eskaliert werden. Zu hoch = schlechte Decision UX. Zu niedrig = verpasste Marge-Chancen.

- **Einbettungsquote:** Anteil Sessions mit gerenderten Experience-Komponenten (3D, AR). Weiterhin relevant, aber nicht mehr einziger KPI.

3.4 Anti-Patterns und Fehlannahmen

Risiko: Typische Organisationsfehler

Anti-Pattern 1: Catalog = nur PIM
Fehlannahme: „Wir haben ein PIM, also sind unsere Daten agent-ready.“ Realität: PIM-Daten sind oft nicht UCP-konform. **Lösung:** Dedicated Catalog Role mit Schema-Validation.
Anti-Pattern 2: Trust als Support-Aufgabe
Fehlannahme: „Trust ist Kundenservice-Thema.“ Realität: Trust Score beeinflusst Agent-Entscheidungen direkt. **Lösung:** Trust als eigene Rolle mit KPI-Verantwortung.
Anti-Pattern 3: Experience = Marketing
Fehlannahme: „3D und AR gehört ins Marketing.“ Realität: Experience Embedding ist technische Integration. **Lösung:** Cross-funktionales Team aus Marketing + Dev.
Anti-Pattern 4: Agent Partnership = IT-Projekt
Fehlannahme: „API-Anbindung ist IT-Sache.“ Realität: Agent Partnership ist Business Development. **Lösung:** Dedizierte Rolle mit P&L-Verantwortung.

3.5 Moat-Bewertungsmatrix

Moat	Aufbaukosten	Zeit	Messgröße	Risiko
Trust Excellence	Mittel	12–24 Mo	Trust Score	Incident-Erosion
Community IP	Hoch	24–36 Mo	Member Count	Plattform-Lock-in
Experience IP	Mittel-Hoch	6–12 Mo	Einbettungsquote	Tech-Obsoleszenz
Exklusive Bundles	Niedrig	3–6 Mo	Bundle AOV	Kopierfähigkeit
Returns Excellence	Mittel	6–12 Mo	Return NPS	Kostenexplosion

Tabelle 7: Moat-Bewertung: Aufwand, Zeit, Messung und Risiken.

Hypothetisches Szenario: Transformierter Modehändler

Hypothetisches Beispiel: Ein mittelständischer Modehändler strukturiert um: 3 Catalog, 4 Experience, 2 Trust, 2 Agent Partnerships. *Annahme nach 12 Monaten:* Signifikanter Agent-Channel-Anteil bei höherem AOV. *Messung:* Order-Attribution via UTM + API-Header.

Handlungsempfehlung: Was du jetzt anders machst

Diese Woche:
- Org-Check: Sind die vier Rollen (Catalog, Experience, Trust, Agent Partnership) besetzt?
- **Erstes Artefakt:** Organigramm-Overlay mit den vier Rollen

Nächstes Quartal:

- Top-3 KPIs pro Rolle implementieren (siehe KPI-Kapitel)
- **Verantwortung:** COO oder VP Operations

Sofort:

- Anti-Pattern-Audit: Fällst du in eines der vier Muster? (Catalog=PIM, Trust=Support, etc.)

4 Agent Negotiation und Policy Files

Wenn du dieses Kapitel überspringst: Agenten verhandeln deine Preise runter, ohne dass du es merkst. Systematisch, über tausende Produkte, 24/7. Ohne Policies bist du dem ausgeliefert.

Definition: Policy Files als Alliance Proposal

Status: Policy Files sind ein **empfohlenes Pattern** (Alliance Proposal), kein standardisiertes Format. AP2 beschreibt Mandates und Audit Trail als Kernmechanik. Visa TAP adressiert Agent-Verifikation. Das hier beschriebene Policy-JSON-Format ist eine kompatible Erweiterung, die diese Konzepte zusammenführt.

4.1 Das Kontrollproblem

Wenn Agenten im Auftrag von Nutzern kaufen, entsteht ein fundamentales Kontrollproblem: Wie stellst du sicher, dass Agenten nicht nur effizient, sondern auch **profitabel und risikominimiert** handeln? Ohne klare Regeln können Agenten Preise drücken, unrentable Deals abschließen oder sogar Fraud ermöglichen.

Policy Files lösen das, indem sie maschinenlesbare Richtlinien definieren, die Agenten vorab prüfen und respektieren müssen. Sie integrieren sich nahtlos in AP2 (Mandates) und Visa TAP (Agent Identity).

4.2 Warum Policies ökonomisch wichtig sind

Policies sind nicht nur technische Hürden – sie sind der **Kern deiner Margenschutzstrategie**. Stell dir vor: Ein Agent verhandelt für einen Kunden über Tausende von Produkten und sucht systematisch nach Rabatten. Ohne Policies könnte das zu einer Erosion deiner Preise führen, da Agenten (z.B. über A2A-Protokolle) untereinander Informationen austauschen könnten.

Ökonomisch gesehen schützen Policies deine Take Rates: In Szenarien mit hoher Agent-Adoption verhindern sie, dass Händler zu reinen Preislieferanten degradiert werden.

Policy Files sind das Äquivalent zu Pricing-, Rabatt- und Channel-Governance im Agent-Zeitalter. Sie definieren nicht nur Sicherheit, sondern Marktpositionierung gegenüber Maschinen.

4.3 Policy-Typen

- **Pricing:** Mindestpreise, Rabattlimits, dynamische Anpassungen

- **Availability:** Lagerbestände, Lieferzeiten, Fallback-Optionen
- **Returns:** Rückgabefristen, Bedingungen
- **Identity:** Verifiable Credentials via AP2 für Fraud-Prävention
- **Geo:** Regionale Beschränkungen
- **Fraud:** Risiko-Scores, Thresholds, Human-Approval bei Hochwertkäufen

4.4 Policy File Konzept (Alliance Proposal)

Hinweis: Dieses Konzept ist ein Alliance Proposal, kein verabschiedeter Standard. Es zeigt, wie maschinenlesbare Händler-Policies mit AP2 Mandates und Visa TAP Agent Identity zusammenspielen könnten.

Kernidee:

- Händler müssen Policies serverseitig enforcen
- Agenten bekommen Ablehnungsgründe maschinenlesbar zurück
- Optional kann es dafür ein Discovery-Manifest geben

Mögliche Discovery: Ein naheliegender Ort wäre `/.well-known/...` im Sinne von RFC 8615. Der finale Pfad ist Teil einer möglichen Standardisierung. Alternativ kann Policy-Discovery als UCP Capability transportiert werden.

Sicherheit: Policies sollten signiert sein (z. B. via JWS im `application/jose+json` Format) und TTL-basiertes Caching unterstützen.

Beispielhafte Regel-Kategorien:

```
{
  "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
  }
}
```

Wichtig: Interne Kalkulationsdaten (wie Margen) sollten nicht exponiert werden. Policies definieren Limits für Agenten, nicht Geschäftsgeheimnisse.

4.5 Threat Model: Angriffsformen und Controls

Policy Files müssen gegen verschiedene Angriffsformen geschützt werden:

1. **Price Scraping plus Cart Stuffing:** Agent sammelt Preise systematisch und nutzt Preisunterschiede. *Control:* Rate Limiting, Agent Identity Verification via Visa Trusted Agent Protocol.

2. **Credential Forgery:** Gefälschte Agent Credentials ermöglichen Massenkäufe. *Control:* Verifiable Credentials in AP2, WebPKI oder DNS-basierte Verifikation.
3. **Replay Attacks:** Alte Policy-Versionen werden wiederverwendet. *Control:* TTL Enforcement, Versionierung mit Semantic Versioning.
4. **Prompt Injection über Produktcontent:** Agent interpretiert Produktbeschreibungen als Anweisungen. *Control:* Structured Data only, Schema Validation via UCP/AXP.
5. **Fraud über Mandate Manipulation:** Manipulierte Mandates umgehen Budget-Limits. *Control:* AP2 Mandate Logik mit Audit Trail, Human Approval bei Thresholds.

4.6 Enforcement: Was passiert bei Policy-Bruch

Bei Verletzung bricht der Prozess ab – der Agent muss entweder anpassen oder abbrechen. Im Worst-Case: Blacklisting des Agents.

Abbildung 9: Policy Discovery Flow: Fetch, Validate, Apply mit drei Endknoten (Accept, Reject, Fallback).

Risiko: Policy-Lücken

Ohne robuste Policies riskierst du Margin Erosion und Fraud. Implementiere mindestens Pricing und Identity Policies vor Agent-Launch.

Handlungsempfehlung: Was du jetzt anders machst

Heute:

- Policy-Audit: Existiert `/.well-known/agent-policy.json`? Wenn nein: anlegen.
- **Erstes Artefakt:** Minimales Policy-File mit Pricing-Rules

Diese Woche:

- Threat-Assessment: Risiko für Price Scraping und Credential Forgery bewerten
- **Verantwortung:** Security + Commerce gemeinsam

Nächste 14 Tage:

- Human-Approval-Schwellen definieren (z.B. >500 EUR = manuell)

5 Die Agentic Commerce Alliance

Wenn du dieses Kapitel überspringst: Standards werden ohne dich gesetzt. Du implementierst später, was andere heute definieren – zu deren Bedingungen.

Die Agentic Commerce Alliance (https://www.agentic-commerce.org) ist die zentrale Industrieinitiative für offene Standards im Agentic Commerce. Gegründet im Juli 2025 unter Führung von Shopware, vereint sie Händler, Technologie-Anbieter, Payment-Provider und KI-Unternehmen weltweit.

5.1 Mission: Human Value Preservation

Die Alliance wurde aus einer strategischen Notwendigkeit geboren: Ohne offene Standards droht ein Szenario, in dem wenige Big-Tech-Plattformen den gesamten Agent-Commerce kontrollieren. Die Mission der Alliance:

1. **Offene Standards:** Entwicklung und Pflege von Protokollen (UCP, AXP, AP2), die nicht von einzelnen Unternehmen kontrolliert werden
2. **Händler-Souveränität:** Sicherstellung, dass Händler Merchant of Record bleiben und Kundendaten nicht an Plattformen abfließen
3. **Interoperabilität:** Vermeidung von Lock-in durch kompatible Protokolle über alle Agent-Surfaces hinweg
4. **Emotionale Wertzonen:** Schutz und Förderung von Bereichen, in denen menschliche Interaktion Mehrwert schafft

5.2 Protokoll-Governance

5.3 Shopware als Founding Member

Shopware spielt als Gründungsmitglied eine zentrale Rolle:

- **AXP-Entwicklung:** Hauptverantwortlich für das Agentic Experience Protocol
- **Referenz-Implementierungen:** SwagUcp-Plugin für Shopware 6 (Open Source)
- **Spatial Commerce:** Integration von 3D/AR-Experiences via AXP
- **PayPal StoreSync:** Deep Integration als Platform-Partner

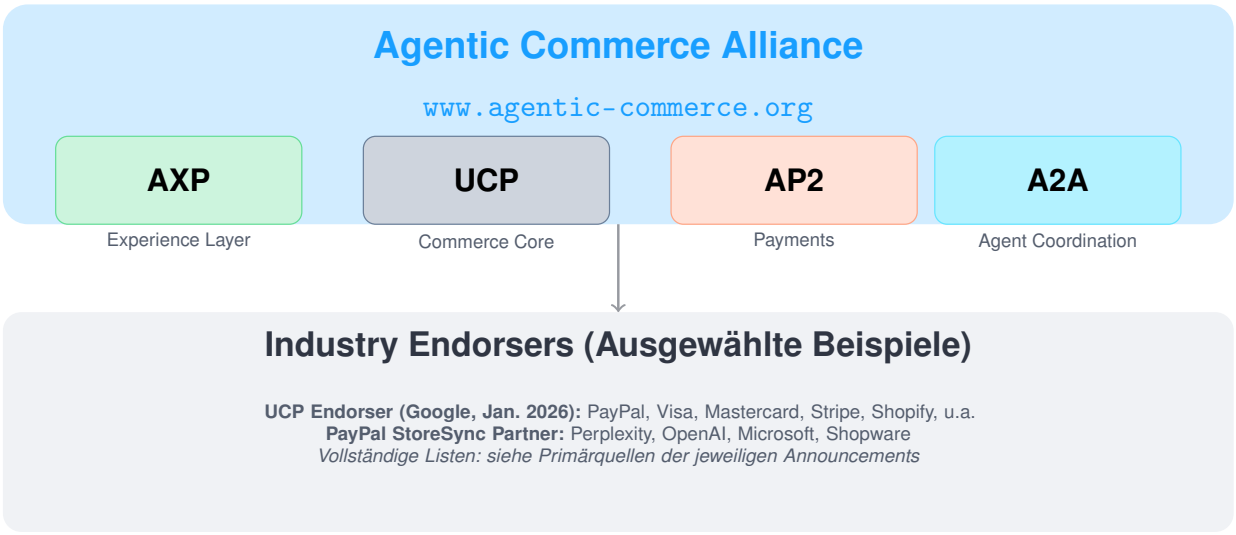

Abbildung 10: Agentic Commerce Alliance: Protokoll-Governance und Industry-Partner.

Handlungsempfehlung: Alliance beitreten

Händler und Technologie-Anbieter können der Alliance unter `https://www.agentic-commerce.org/join` beitreten. Vorteile: Mitgestaltung der Standards, früher Zugang zu Protokoll-Updates, Networking mit Industry Leaders.

Implikationen nach Zielgruppe – Teil II

Wenn du Händler bist:

- Deine Organisation braucht die vier Rollen: Catalog, Experience, Trust, Agent Partnership
- Policy Files sind Margenschutz, nicht Bürokratie – implementiere sie vor Agent-Launch
- Miss die neuen KPIs: Agent Adoption, Trust Score, Policy Abort Rate
- **No-Go:** Behandle Agent Partnership nicht als IT-Projekt – es ist Business Development

Wenn du Plattform bist:

- Unterstütze Händler beim Aufbau der vier Rollen mit Tools und Templates
- Policy-Infrastruktur ist strategisch – biete einfache Policy-File-Generation an
- Integriere KPI-Dashboards für Agent-Metriken in deine Analytics
- **No-Go:** Verzögere nicht die Alliance-Teilnahme – Standards werden jetzt gesetzt

Wenn du Investor bist:

- Due Diligence muss Operating Model für Agentic Commerce abfragen
- Portfolio-Unternehmen brauchen Policy-Readiness und KPI-Tracking
- Alliance-Mitgliedschaft ist positives Signal für Protokoll-Readiness
- **No-Go:** Investiere nicht in Unternehmen, die Agent-Channel als „später“ einordnen

TEIL III

Technologie & Strategie

6 Protokoll-Landkarte Q1 2026

Wenn du dieses Kapitel überspringst: Du triffst Build-vs-Buy-Entscheidungen blind. Du baust, was du kaufen solltest, und kaufst, was du bauen müsstest. Beides kostet dich 6–12 Monate.

Dieses Kapitel gibt einen Überblick über die aktuelle Protokoll-Landschaft im Agentic Commerce. Wichtig: Kein Protokoll ersetzt ein anderes. Sie adressieren unterschiedliche Schichten desselben agentischen Kaufprozesses und bilden zusammen einen interoperablen Agentic-Commerce-Stack mit komplementären Protokollen.

6.1 Das Master-Stack-Diagramm

Dieses Diagramm ist die zentrale Referenz für alle Protokoll-Diskussionen in diesem Strategiebuch. Alle späteren Kapitel beziehen sich auf diese fünf Ebenen.

6.2 Ebene 1: Core Commerce

UCP (Universal Commerce Protocol): End-to-End-Commerce-Protokoll für Discovery, Capability Description, Order und Checkout-Orchestrierung. Von Google als offener Standard lanciert (11. Januar 2026), endorsed by more than 20 others. Definiert eine offene, gemeinsame Sprache für Agenten, Händler-Backends, Plattformen und Zahlungsdienste über den gesamten Kaufprozess – von Discovery über Bestellung bis Post-Purchase. Kompatibel mit AP2 (Zahlungsmandate), A2A (Agent-zu-Agent-Kommunikation) und MCP (Kontext-/Daten-Transport).

ACP (Agentic Commerce Protocol): Offener, produktiv eingesetzter Checkout-Standard für agentische Kaufabschlüsse (Instant Checkout). Apache 2.0 lizenziert, von OpenAI und Stripe maintainted. Optimiert für agentengesteuerte Checkout-Flows mit Shared Payment Tokens und Merchant-of-Record-Modell. Basis für OpenAI Instant Checkout in ChatGPT. Wird von Microsoft als „offener Standard“ referenziert.

6.3 Ebene 2: Payments & Trust

AP2 (Agent Payments Protocol): Standard für Payment Mandates und sichere, kryptographisch belegbare Agent-Zahlungsautorisierung. Von Google dokumentiert als offenes Agent Payments Protocol. Definiert Zahlungsmandate und Autorisierung für Agent-Transaktionen. Kompatibel mit UCP und für UCP-Flows vorgesehen.

Visa Trusted Agent Protocol (TAP): Von Visa vorgestellt (14. Oktober 2025). Adressiert Agent Identity, Consumer Recognition, Payment Information. Ergänzt andere Protokolle wie ACP und

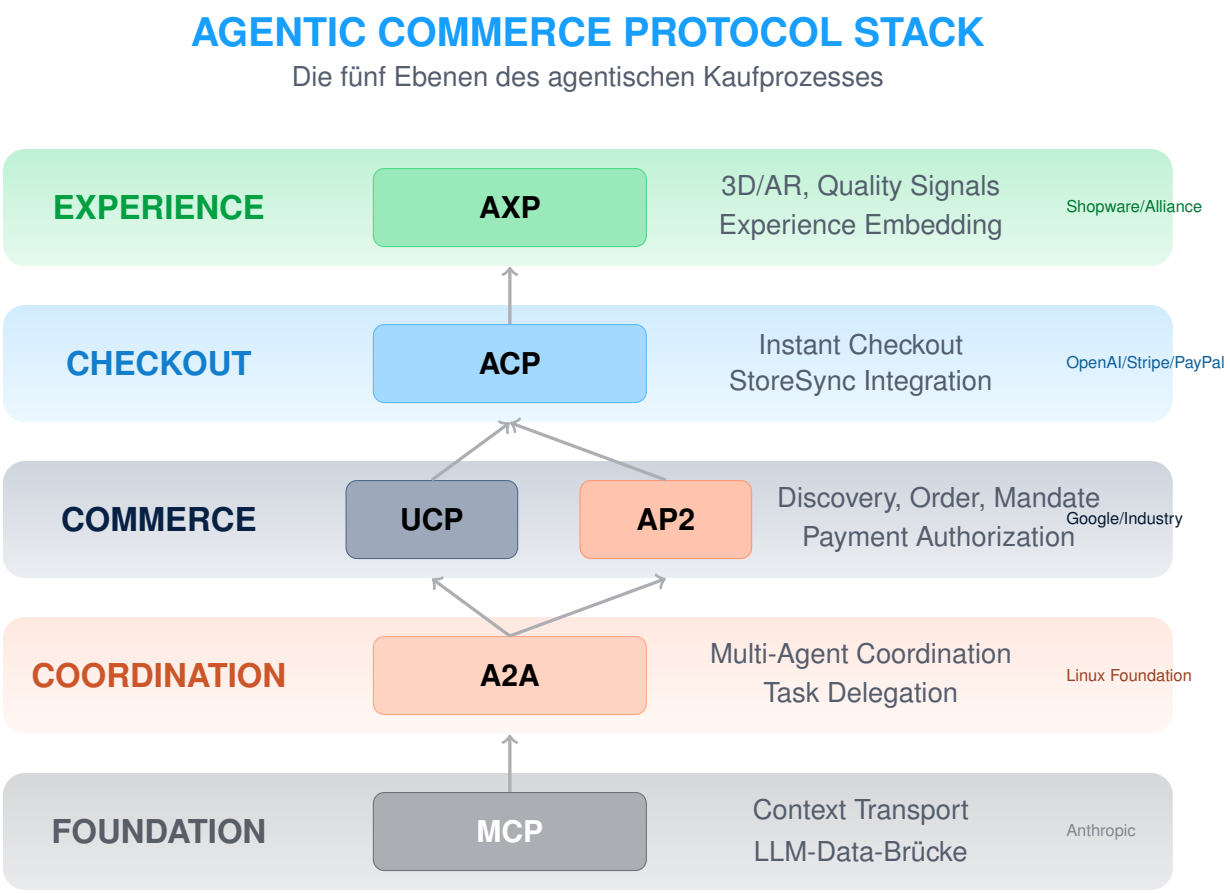

Abbildung 11: Master-Stack-Diagramm: Die fünf Ebenen des Agentic Commerce. MCP als Integrationsschicht, darauf A2A (Coordination), UCP/AP2 (Commerce), ACP (Checkout), AXP (Experience). Dieses Diagramm ist die zentrale Referenz.

AP2 im Trust-Layer.

6.4 Ebene 3: Agent Coordination & Context

A2A (Agent2Agent Protocol): Ermöglicht Multi-Agent-Szenarien und Agent-zu-Agent-Kommunikation. Wird von UCP für komplexe Orchestrierungen genutzt.

MCP (Model Context Protocol): Basis-Kontexttransport für Agent-Kommunikation, produktionsreif. Ermöglicht Kontext-/Daten-Transport zwischen Agenten und Services.

6.5 Ebene 4: Experience Layer

AXP (Agentic Experience Protocol): Von Shopware und der Agentic Commerce Alliance entwickelt. Erweitert UCP um drei Kernfähigkeiten:

1. **Product Data:** Strukturierte Produktinformationen für komplexe Typen (Varianten, Konfiguratoren, Events, Subscriptions, Bundles)
2. **Quality Data:** Trust-Signale inkl. Reviews, Returns, Intent Information, Merchant Reputation
3. **Experience Embedding:** Sandboxed Live-Experiences von Händlern (3D-Viewer, Konfiguratoren, AR)

AXP Capabilities:

- `dev.axp.product_data` – Basis-Produktdaten
- `dev.axp.product_data.variants` – Varianten-Support
- `dev.axp.product_data.configurator` – Komplexe Konfiguratoren
- `dev.axp.quality_data.reviews` – Reviews und Ratings
- `dev.axp.quality_data.trust` – Merchant und Product Trust
- `dev.axp.experience_embedding.viewer_3d` – 3D-Viewer
- `dev.axp.experience_embedding.ar` – Augmented Reality
- `dev.axp.decision_metadata` – Strukturierte Entscheidungshilfen (Vergleiche, Filter, Empfehlungslogik)
- `dev.axp.trust_presentation` – Trust-Signal-Präsentationshinweise für Agent-Surfaces
- `dev.axp.escalation_hooks` – Human-Handover-Trigger und Eskalationsschwellen

Wichtig: AXP ist nicht nur ein Media-Protokoll für 3D/AR, sondern ein umfassendes Experience-Transport-System. Die neuen Capabilities (`decision_metadata`, `trust_presentation`, `escalation_hooks`) ermöglichen Händlern, Entscheidungslogik und Trust-Inszenierung als maschinenlesbare Hinweise zu liefern, nicht nur als visuelle Assets.

Deployment: AXP kann als UCP-Addon (`/.well-known/ucp`) oder standalone (`/.well-known/axp`) deployed werden.

Policy Files: Maschinenlesbare Richtlinien unter `/.well-known/agent-policy.json`, integrieren sich in ACP und AP2. Definieren Pricing-, Rabatt- und Channel-Governance im Agent-Zeitalter.

6.6 Ebene 5: Commerce Enablement Services

PayPal StoreSync: PayPals Flaggschiff-Service für Agentic Commerce. Macht Händler-Produktdaten in führenden AI-Channels auffindbar und orchestriert den gesamten Cart-Lifecycle.

StoreSync-Komponenten:

- **Product Feed Integration:** Automatische Synchronisation von Produkt-Katalogen. Near-Realtime Inventory, Pricing, Attribute. Unterstützt Google Shopping CSV Format.
- **Cart Orchestration:** Komplette Shopping-Journey von Discovery bis Checkout. AI-Agents können Carts erstellen, Coupons anwenden, Shipping-Optionen handhaben.
- **Headless Checkout:** Integration mit jeder AI-Surface ohne Redirect.

StoreSync-Partner:

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

Merchant Value: Händler bleiben Merchant of Record, behalten Kundenkontakt und Brand-Visibility. Eine PayPal-Integration ermöglicht Präsenz auf allen AI-Surfaces.

Experience Embedding: Security und Compliance Boundaries

AXP Experience Embedding (3D, AR, Konfiguratoren) folgt strikten Sicherheitsrichtlinien:

- **No Full Page Takeover:** Embedded Experiences dürfen nicht das gesamte Agent-Interface übernehmen. Maximale Viewport-Fläche: 60% (empfohlen).

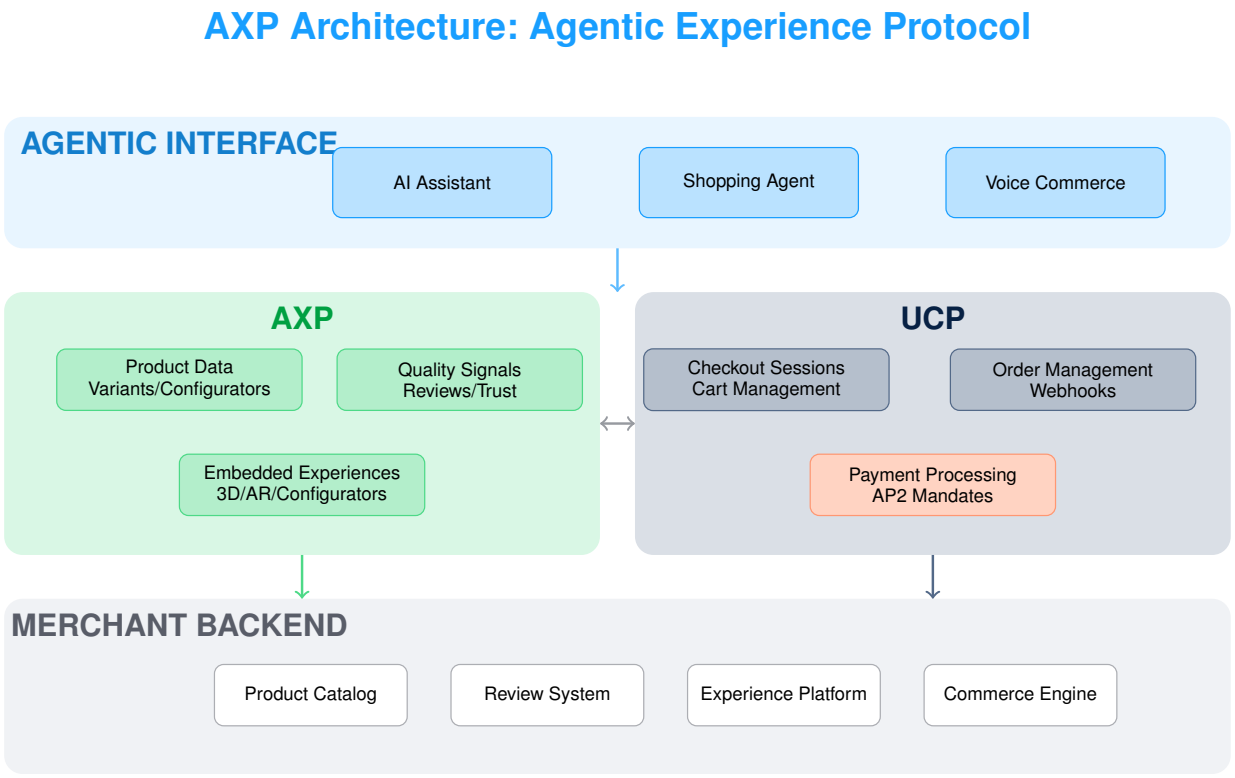

Abbildung 12: AXP Architecture: Das Agentic Experience Protocol erweitert UCP um strukturierte Produktdaten, Quality Signals und Embedded Experiences. Beide Protokolle kommunizieren über standardisierte Schnittstellen.

- **No Uncontrolled Scripts:** Sandboxed Execution via iFrame mit Content Security Policy (CSP). Kein Zugriff auf Agent-Context oder Nutzerdaten außerhalb des Embeddings.
- **Deterministic UX Boundaries:** Klare Abgrenzung zwischen Agent-Oberfläche und Händler-Embedding. Nutzer muss jederzeit erkennen, wer welchen Teil kontrolliert.

Rationale: Diese Boundaries schützen Nutzer vor Phishing, Fraud und Dark Patterns. Sie erlauben Händlern differenzierte Experiences, ohne Agent-Plattformen in Haftungsrisiken zu bringen. Compliance-Teams und Security-Verantwortliche können beruhigt Experience Embedding freigeben.

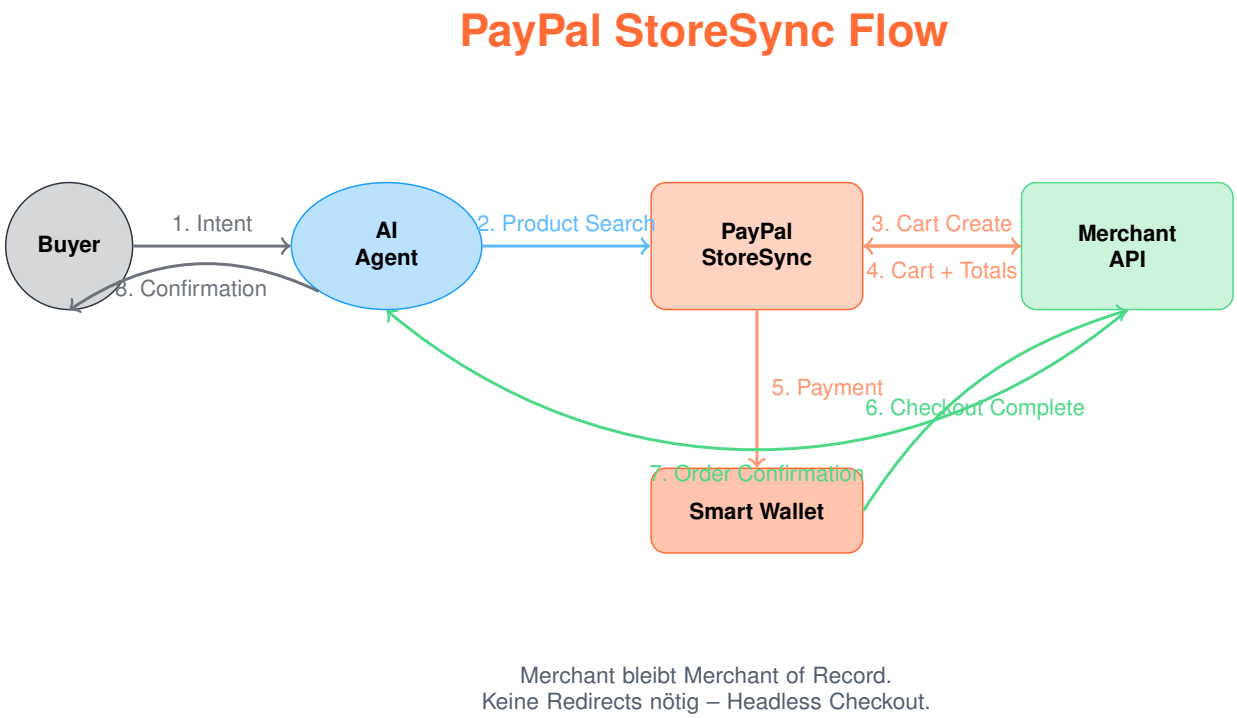

Abbildung 13: PayPal StoreSync Flow: Von Buyer Intent bis Order Confirmation. Der Agent kommuniziert mit PayPal StoreSync, das die Cart-Orchestrierung übernimmt. Smart Wallet ermöglicht nahtlosen Checkout ohne Redirects.

7 Der Agentic Commerce Tech-Stack

7.1 Protokoll-Stack: Detailansicht

Die Protokolle bilden einen interoperablen Stack mit klarer Schichtung (siehe Master-Stack-Diagramm auf Seite 32). Jede Ebene adressiert spezifische Anforderungen des agentischen Kaufprozesses:

- **Foundation (MCP):** Basis-Kontexttransport zwischen LLMs und externen Datenquellen
- **Coordination (A2A):** Multi-Agent-Szenarien und Task-Delegation
- **Commerce (UCP/AP2):** Discovery, Order-Management und Payment-Autorisierung
- **Checkout (ACP):** Instant-Checkout-Flows und StoreSync-Integration
- **Experience (AXP):** 3D/AR, Quality Signals und Experience Embedding

7.2 Protokoll-Übersicht

Hinweis zur Architektur: Die Protokolle bilden zusammen einen interoperablen Stack. UCP orchestriert den gesamten Commerce-Flow inklusive Purchase und Order Management. AP2 ist als kompatible Payments-Schicht vorgesehen. ACP ist eine alternative Checkout-Implementierung (OpenAI/Stripe). A2A und MCP sind Ergänzungen für Agent-Coordination und Context-Transport.

Protokoll	Funktion	Ökon. Bedeutung	Status Q1/26
UCP	End-to-End Commerce inkl. Checkout	Standardisierung senkt Kosten	Initial Release[1]
ACP	Instant Checkout (Alternative)	Schnelle Checkout-Integration	Draft (Spec)[2]
AP2	Payment Mandates & Autorisierung	Sichere Agent-Zahlungen	Initial Release[3]
Visa TAP	Trust & Identity	Agent-Verifikation	Verfügbar[4]
A2A	Agent-Coordination	Multi-Agent-Szenarien	Frühe Adoption
MCP	Context-Transport	Basis Agent-Kommunikation	Produktiv[5]
AXP	Experience Layer	Rich Content in Agents	Alliance Proposal

Tabelle 8: Protokoll-Status Q1/2026. **Verfügbar** = Spezifikation veröffentlicht, erste Implementierungen. **Initial Release** = Veröffentlichte Spezifikation. **Draft** = Spezifikation in Entwicklung.

7.3 Zwei Checkout-Pfade im Agentic Commerce

Google beschreibt UCP als Standard für die gesamte Commerce Journey, inklusive Purchase und Order Management. ACP (OpenAI/Stripe) fokussiert auf Instant Checkout. Beide Ansätze

existieren parallel im Markt:

Aspekt	Pfad 1: UCP + AP2 (Google)	Pfad 2: ACP (OpenAI/Stripe)
Scope	End-to-End: Discovery bis Order	Fokus: Instant Checkout
Payment	AP2 Mandates integriert	Shared Payment Tokens
Endorser	Google, PayPal, Visa, 20+ Partner	OpenAI, Stripe, Microsoft
Best für	Full-Stack-Integration	Schneller Checkout-Launch

Tabelle 9: Zwei dominante Checkout-Varianten. Du musst nicht wählen – beide sind kompatibel und können parallel implementiert werden.

7.4 So kauft ein Agent: Sequenzdiagramm

Hinweis: Die Protokolle arbeiten zusammen in einem interoperablen Stack. UCP orchestriert den gesamten Flow, AP2 sichert Zahlungsautorisierung, ACP ermöglicht Instant Checkout-Flows.

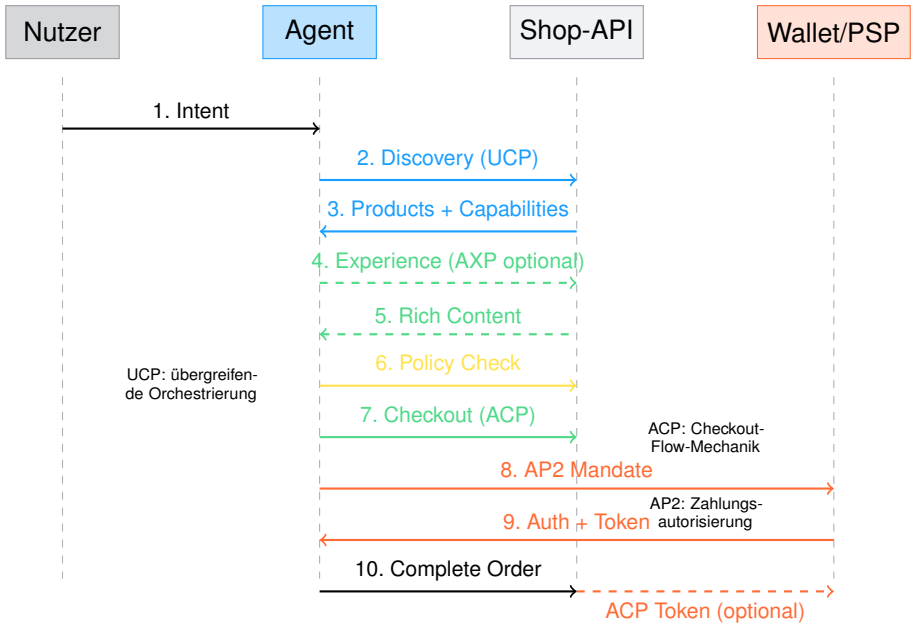

Abbildung 14: Kaufprozess im interoperablen Protokoll-Stack mit optionalen Branches.

7.5 Eigenentwicklung vs. Partner

Komponente	Eigenentwicklung	Partner
UCP-Integration	Nur bei sehr spezifischen Needs	Empfohlen: Plattform-Plugins
Agent-Gateway	Bei >10 Agent-Integrationen	Empfohlen: StoreSync o.ä.
Experience-Engine	Bei einzigartiger UX-Vision	3D: diverse Anbieter
Trust-Aggregation	Selten sinnvoll	Meist Partner

Tabelle 10: Eigenentwicklung vs. Partner: Empfehlungen.

8 Erlebnisplattform

Wenn du dieses Kapitel überspringst: Du wirst zum Standardprodukt. Agenten vergleichen dich nur noch über Preis und Lieferzeit. Deine Marke, dein Content, deine UX – für Agenten unsichtbar.

Die Erlebnisplattform ist der Differenzierer in Agentic Commerce: Während Agenten Standardkäufe automatisieren, gewinnen Händler durch strukturierte Entscheidungshilfen, Trust-Inszenierung und immersive Erlebnisse. Basierend auf dem Agentic Experience Protocol (AXP) transportiert sie nicht nur Rich Content, sondern das gesamte Decision und Trust Operating System.

8.1 Warum Erlebnisplattformen entscheidend sind

Agenten optimieren auf Effizienz, aber Entscheidungen brauchen Struktur und Vertrauen. Erlebnisplattformen wirken auf drei Ebenen:

- **Decision Experience:** Strukturierte Vergleiche, Filter und Empfehlungen reduzieren Komplexität für Agenten und Menschen
- **Trust Experience:** Präsentation von Quality Signals als erlebbare Sicherheit, nicht nur als Datenpunkte
- **Immersive Experience:** 3D-Viewer, AR und Konfiguratoren für sensorische und emotionale Differenzierung

Wichtig: Die meisten Händler starten bei Level 3 (Immersive), obwohl Level 1 (Decision) und Level 2 (Trust) schneller Wert liefern und günstiger zu implementieren sind.

Conversion Uplift durch Experience Embedding:

15–25% *(Szenario basierend auf AR-Benchmarks und Pilotprojekten)*

- **Baseline:** Conversion Rate ohne Experience Embedding (Agent-Orders, Kategorie-spezifisch)
- **Segmentierung:** Fashion, Möbel, Elektronik profitieren stärker als Commodities
- **Kritischer Faktor:** Load Time <2s, sonst killt Latenz den Effekt
- **Messung:** A/B Test mit/ohne Embedding, Attribution via UTM + API-Header

Die Kernfrage: **Was kann ein Agent nicht alleine liefern?** Die Antwort: Sensorische, emotionale, identitätsstiftende Erlebnisse.

8.2 Konkrete Muster

AR Viewer: Nutzer „probieren“ Produkte virtuell – Möbel im Raum, Brillen im Gesicht. In AXP: Sandboxed Embedding.

3D Configurator: Kunden bauen Produkte selbst. Real-time Pricing via AXP.

Guided Selling: Agent-geführte Beratung mit Präferenz-Matching.

Community Loops: User-Generated Content in AXP Quality Data.

Service Bundles: Käufe mit Add-ons: Installation, Garantie.

Returns as Trust Lever: Simulierte Rückgaben via AXP bauen Vertrauen.

Handlungsempfehlung: Erlebnisplattform aufbauen

Diese Woche: Wähle eine Kategorie mit hohem Sensorik-Bedarf (Fashion, Möbel, Elektronik).
Nächste 30 Tage: AR-Pilot live, Einbettungsquote messen.
Ziel Q1: 10% Einbettungsquote, erste Conversion-Daten.
Verantwortung: Experience-Team (nicht Marketing allein).

Handlungsempfehlung: Was du jetzt anders entscheiden solltest

- **Kategorie-Auswahl:** Identifiziere die Kategorie mit höchstem Experience-Potenzial
- **Tech-Stack:** Evaluiere 3D/AR-Provider für AXP-Kompatibilität
- **Messbarkeit:** Definiere Einbettungsquote und Conversion-Uplift-Baseline vor Pilot-Start

9 KPIs im Agentic Commerce

Wenn du dieses Kapitel überspringst: Du misst weiter Conversion Rate und Page Views, während die echten Hebel – Agent Adoption, Trust Score, Policy Abort Rate – im Dunkeln bleiben. Du steuerst mit veralteten Instrumenten.

9.1 KPI-Definitionen mit Formeln

KPI	Formel/Definition	Frequenz	Verantwortlich
Data Fill Rate	Pflichtfelder / Gesamt $\times$ 100	Täglich	Catalog
Update Speed	Median(Sync-Zeit) in Minuten	Real-time	Catalog
Agent Adoption	Agent-Orders / Alle Orders $\times$ 100	Wöchentlich	Agent Partnership
Agent Conversion	Agent-Completed / Agent-Initiated	Wöchentlich	Agent Partnership
Trust Score	Trust Index 0–100	Monatlich	Trust
Policy Abort Rate	Abbrüche / Agent Requests	Real-time	Trust

Tabelle 11: KPI-Definitionen: Diese Tabelle zeigt die sechs Kern-KPIs – damit du weißt, was du messen musst, um Agent-Readiness zu steuern.

Definition Agent Order: Order initiiert durch Agent mittels standardisierter Agent-Credential Headers/Token (verifizierte Agent-Identity). Empfehlung: Agent Orders markieren über standardisierte Request Metadaten, zum Beispiel signierte Agent Credentials oder Gateway Header. Feldname ist Implementierungsdetail (z.B. `X-Agent-ID` Header oder Agent-Referrer).

9.2 KPI-Implementation: Stack-Signal und System of Record

Praktische Hinweise:

- **Multi-Agent-Szenarien:** Bei A2A-Flows kann eine Order mehrere Agenten involvieren. Attribution an den initiierenden Agent via `primary_agent_id`.
- **Retry-Handling:** AP2 Mandates sind idempotent. Verwende `mandate_id` als Deduplizierungsschlüssel.
- **Cross-System-Sync:** Trust Score aggregiert aus mehreren Quellen (Reviews, Returns, Incidents). Definiere klare Update-Frequenzen und Konfliktauflösung.

KPI	Stack-Signal	System of Record	Deduplizierung
Agent Adoption	AP2 Mandate Event	Order-System	Idempotency Key pro Mandate
Trust Score	AXP Quality Signals	Trust-Aggregator	Zeitstempel + 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

Tabelle 12: KPI-Implementation: Diese Tabelle zeigt, wo das Signal entsteht, wer System of Record ist und wie du deduplizierst – damit du Montag mit der Implementierung starten kannst.

Handlungsempfehlung: Was du jetzt anders machst

Diese Woche:

- Agent Adoption und Trust Score ins Exec-Dashboard
- **Erstes Artefakt:** Dashboard-Widget mit zwei neuen KPIs

Nächste 14 Tage:

- Agent-Order-Tracking via `X-Agent-ID` Header implementieren
- **Verantwortung:** Engineering + BI gemeinsam

Nächste 30 Tage:

- Alerts: Policy Abort Rate >5%, Price Mismatch >1%

9.3 Zielwerte nach Kategorie (Szenario)

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+

Tabelle 13: Zielwerte nach Kategorie (Szenario 2030). *Alle Werte sind illustrative Annahmen basierend auf Automatisierbarkeit und Kategoriecharakteristik – keine Prognosen.

10 Strategische Roadmap

Wenn du dieses Kapitel überspringst: Du startest ohne Gates. Du skalierst, bevor der Pilot funktioniert. Oder du wartest zu lange und verpasst das Zeitfenster, in dem First Mover noch Vorteile haben.

10.1 Phasen mit wirtschaftlichen Gates

Phase	Zeitraum	Aktivitäten	Success Gate	Wirtsch. Gate
Audit	Mo 1–3	Data Audit, API-Check	Readiness Score	Budget OK
Pilot	Mo 4–6	1 Agent, 1 Kategorie, **Decision UX**	Erste Orders	CAC neutral
Scale	Mo 7–12	Multi-Agent, **Hybrid Experience**	20%+ Agent	Margin stabil
Optimize	Mo 13+	**Immersive Experience**, A/B	Profitabilität	CM positiv

Tabelle 14: Roadmap mit wirtschaftlichen Gates: CAC, Margin, Contribution Margin.

Experience-Fokus pro Phase:

- **Pilot Phase:** Decision UX – Strukturierte Vergleiche und Entscheidungshilfen ohne teure AR-Produktion. Ziel: Conversion-Baseline etablieren.
- **Scale Phase:** Hybrid Experience – Trust-Signal-Präsentation und Human-Handover-Trigger. Ziel: Assisted Conversion Rate >15%.
- **Optimize Phase:** Immersive Experience – 3D, AR, Konfiguratoren für High-Value-Kategorien. Ziel: Marge-Verteidigung gegen Standardanbieter.

Kritisch: Händler, die sofort mit AR starten, überspringen Decision und Trust Experience. Resultat: Hohe Kosten, aber keine Conversion-Verbesserung, weil die Entscheidungslogik fehlt.

10.2 Capability Ladder

1. **Level 1 – Data Readiness:** Vollständige, UCP-konforme Produktdaten
2. **Level 2 – Trust Signals:** Reviews, Zertifikate, Return-Policies maschinenlesbar
3. **Level 3 – Agent-Kanäle:** Erste API-Anbindungen, Policy Files live
4. **Level 4a – Decision Experience:** Strukturierte Vergleiche, Filter, Entscheidungshilfen via AXP Decision Metadata
5. **Level 4b – Trust Experience:** Trust-Signal-Präsentation, Human-Handover-Trigger via AXP Trust Presentation

6. **Level 4c – Immersive Experience:** AR, 3D, Konfiguratoren via AXP Experience Embedding
7. **Level 5 – Multi-Agent:** Orchestrierung mehrerer Agents, B2B-Szenarien

Wichtig: Händler müssen *nicht* mit Level 4c (AR/3D) starten. Level 4a (Decision Experience) liefert bereits messbaren Wert durch bessere Entscheidungsreduktion – ohne teure 3D-Produktion. Level 4b (Trust Experience) erhöht Conversion durch bessere Trust-Inszenierung. Level 4c ist die Kür, nicht die Pflicht.

11 Risiken und Controls

Risiken im Agentic Commerce sind vielfältig, aber beherrschbar. Dieses Kapitel erweitert die Risk-Control-Matrix um hypothetische Incident-Patterns, spezifische Controls und Haftungsfragen.

11.1 Hypothetische Incident-Patterns

Hypothetisches Szenario: Halluzinations-Risiko

Hypothetisches Beispiel: Ein Agent könnte falsche Produktverfügbarkeit „halluzinieren“, was zu überbuchten Beständen führt. *Potenzielle Folge:* Erhöhte Rücklaufquote, Kosten. *Gegenmaßnahme:* Structured Data enforced via UCP.

Hypothetisches Szenario: Unauthorized Buy Risiko

Hypothetisches Beispiel: Ein Agent kauft ohne Budget-Check, da Identity-Policy fehlt. *Potenzielle Haftung:* Wallet-Provider (AP2) oder Händler. *Gegenmaßnahme:* Thresholds in Policies.

Hypothetisches Szenario: Fraud-Angriffs-Vektor

Hypothetisches Beispiel: Gefälschte Credentials ermöglichen Massenkäufe. *Gegenmaßnahme:* Verifiable Credentials in AP2, Anomaly Detection.

11.2 Risk-Control-Matrix

11.3 Haftungsverteilung

- **Agent-Provider:** Haftet bei Protokoll-Fehlern
- **Händler:** Haftet bei Policy-Lücken und unzureichenden Daten
- **Wallet-Provider:** Haftet bei Payment-Fehlern innerhalb AP2
- **Nutzer:** Final verantwortlich für Agent-Autorisierung

Risiko: Unkontrollierte Risiken

Jeder Vorfall senkt deinen Trust Score. Implementiere proaktive Controls vor Agent-Launch.

Risiko	Control	Protokoll	Verantwortlich	Monitoring
Halluzination	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 Det.
Liability Gap	Klare AGB, Insurance	Legal	Legal	Incident Log
Data Breach	Consent, Encryption	MCP/UCP	Trust	Quartals-Audit

Tabelle 15: Risk-Control-Matrix mit detaillierten Controls.

12 Gewinner und Verlierer

Dieses Kapitel analysiert, welche Akteure im Agentic Commerce gewinnen und welche verlieren – basierend auf konkreten Mechanismen der Wertverschiebung, nicht auf Spekulation.

12.1 Mechanik: Wer besitzt was?

Die Wertverschiebung hängt von vier Schlüsseln ab. Wer diese kontrolliert, gewinnt. Wer sie ignoriert, verliert.

12.1.1 Distribution besitzen

Gewinner: Protokollfähige Händler mit UCP-Integration, die ihre Produktdaten maschinenlesbar und aktuell halten. *Mechanik:* Agenten scannen via UCP – beste Daten gewinnen. Händler mit vollständigen, strukturierten Daten werden häufiger gefunden und gekauft.

Verlierer: SEO-abhängige Händler ohne Protokoll-Anbindung. *Mechanik:* Klassische Suchmaschinen verlieren an Bedeutung. Wer nur auf Google-Rankings setzt, verliert Agent-Traffic.

Handlungsempfehlung: UCP-Compliance ist keine Option, sondern Voraussetzung. Investition in Datenqualität zahlt sich direkt in Agent-Reichweite aus.

12.1.2 Wallet besitzen: Das PayPal-Paradigma

Gewinner: Wallets mit AP2-Integration (z. B. PayPal, Apple Wallet). *Mechanik:* In der Vergangenheit authentifizierte der Nutzer jeden Kauf („Click to Pay“). Im Jahr 2026 authentifiziert der Nutzer den *Agenten* einmalig.

PayPal hat diesen Shift mit der Öffnung der **„Identity-for-Agents“ Infrastruktur** (September 2025) gewonnen. Sie lösen das sogenannte „M×N Problem“ (M Agenten interagieren mit N Händlern), indem sie Agenten eine verifizierbare, kryptographische Identität geben.

PayPal Agentic Commerce Services:

- **StoreSync:** Produkt-Feed-Integration und Cart-Orchestrierung
- **Smart Wallet:** Vaulted Payment Experience ohne Redirects
- **400M+ Active Accounts:** Globale Reichweite in 200+ Märkten
- **25+ Jahre Trust:** Fraud Prevention, Identity Verification, Buyer-Seller Protection

Verlierer: Banken und PSPs, die auf 3D-Secure und manuellen 2-Faktor-Checks beharren. Diese brechen autonome Agent-Flows und führen zu „Cart Abandonment by Bot“.

Handlungsempfehlung: Action für Händler

Aktiviere „Agentic Payments“ in deinem PSP-Backend. Stelle sicher, dass dein Checkout PayPal AP2-Tokens akzeptiert – sonst blockierst du Instant-Orders von ChatGPT, Microsoft Copilot und Google Shopping Agent.

12.1.3 Trust besitzen

Gewinner: Aggregatoren mit Quality Signals via AXP, verifizierte Trust Scores. *Mechanik:* Agenten nutzen Trust Scores für Entscheidungen. Händler mit hohen, verifizierten Scores werden bevorzugt.

Verlierer: Isolierte Silos ohne Trust-Signal-Integration. *Mechanik:* Agenten können isolierte Reviews nicht aggregieren. Wer keine maschinenlesbaren Trust-Signale liefert, wirkt weniger vertrauenswürdig.

Handlungsempfehlung: Trust-Signale müssen maschinenlesbar sein. Returns Excellence, Incident-Historie, Verifikation – alles muss via AXP kommunizierbar sein.

12.1.4 Experience Layer besitzen

Gewinner: AR/3D-Tools via AXP, Embedded Experiences. *Mechanik:* Erlebnisplattformen erhöhen Conversion signifikant. Händler mit Rich Content gewinnen gegen Standardanbieter.

Verlierer: Statische Shops ohne Experience-Komponenten. *Mechanik:* Agenten können Standard-Produktdaten liefern. Wer keine differenzierenden Experiences bietet, wird zum Standardprodukt.

Handlungsempfehlung: Start mit AR-Pilot in einer Kategorie. Messen: Einbettungsquote und Conversion-Uplift. Target: 10% Einbettungsquote nach 3 Monaten.

12.2 Wertverschiebung: Konkrete Zahlen (Szenario-Hypothesen)

Segment	Gewinner	Verlierer	Take Rate Shift	Status
Payments	**Agent-Wallets** (AP2)	Legacy Checkout	+0.5–1% neu	Hypothese*
Auffindbarkeit	**Protokollfähige** (UCP)	SEO-abhängige	2–5% neu	Hypothese*
Experience	**AR/3D-Tools** (AXP)	Static Content	10–20% Uplift	Hypothese*
Data	Signal-Aggregatoren	Review-Silos	0.1–0.5% neu	Hypothese*

Tabelle 16: Wertverschiebung (Szenario 2030). Diese Tabelle zeigt, welche Akteure in welchen Segmenten profitieren – damit du Investitionsprioritäten setzen kannst. *Hypothese = illustrative Annahme, keine Prognose.

Begründung Take Rates:

- *Auffindbarkeit:* Agenten monetarisieren Empfehlungen (ähnlich Affiliate)
- *Experience:* Conversion-Uplift rechtfertigt Premium-Pricing

- *Payments:* Wallet-Provider können bei Agent-Transaktionen Fees erheben

These: Gewinner 2030

Gewinner kontrollieren Protokolle und Experiences. Verlierer ignorieren den Shift.

Implikationen nach Zielgruppe – Teil III

Wenn du Händler bist:

- UCP-Compliance ist Pflicht, AXP-Experience ist Kür – beides ist nötig
- Entscheide Build vs. Buy anhand deiner Kernkompetenz (meist: Buy für Protokolle)
- Nutze PayPal StoreSync als schnellen Einstieg in Agent-Surfaces
- **No-Go:** Baue keine proprietären Agent-APIs – das skaliert nicht

Wenn du Plattform bist:

- Protokoll-Referenzimplementierungen sind strategisch (vgl. SwagUcp)
- Erlebnisplattform als Differenzierungsmerkmal für deine Kunden
- Integriere StoreSync und ähnliche Services für schnelle Agent-Anbindung
- **No-Go:** Konkurriere nicht gegen offene Standards – kooperiere

Wenn du Investor bist:

- Protocol-Stack-Position im Mental Model zeigt strategische Relevanz
- Wallet-Position (PayPal, Apple) ist hochwertig – hohe Switching Costs
- Experience-Tech-Startups profitieren vom AXP-Standard
- **No-Go:** Unterschätze nicht die Geschwindigkeit der Adoption – produktive Systeme existieren heute

Epilog: Der letzte Händler – Fortsetzung

Fünf Jahre später. Derselbe Morgenspaziergang, dieselbe Straße.

Der „letzte Händler“ ist immer noch da – aber nicht mehr allein. Sein Laden ist jetzt ein Experience Hub. Kunden kommen zum Anfassen, Erleben, zur Community. Die Transaktionen laufen über Agenten – aber sein Trust Score ist der höchste, seine Daten die besten, seine Experiences die differenziertesten.

Drei Türen weiter hat ein junger Händler eröffnet. Er hat nie SEO betrieben, nie Ads geschaltet. Sein gesamtes Geschäft läuft über Agent-Kanäle. Er nennt es „protokollfähig“.

Die Moral: Der Handel stirbt nicht. Er transformiert sich. Die Gewinner verstehen, dass Agenten der effizienteste Vertriebskanal sind – wenn du weißt, wie du ihn bespielst.

These: Handel 2030

Handel 2030 = Mensch $\times$ KI. Der Multiplikator entscheidet.

Die drei Währungen – ein letztes Mal:

- **Protokolle** sichern Sichtbarkeit. Ohne UCP, AXP, AP2 existierst du für Agenten nicht.
- **Trust** sichert Auswahl. Agenten bevorzugen verifizierte, zuverlässige Händler.
- **Experience** sichert Marge. Wer nur Daten liefert, wird zum Standardprodukt. Wer Erlebnisse bietet, bleibt differenziert.

Das ist die Leitthese dieses Strategiebuchs. Alles andere folgt daraus.

Klarstellung: Agentic Commerce ist kein Zukunftsmärchen, sondern eine operative Realität mit klaren KPIs, Risiken und Investitionsentscheidungen. Die Einführungsphase läuft bereits (2024–2026), produktive Agent-Checkouts existieren heute.

Glossar

A2A
Agent2Agent Protocol – Kommunikation zwischen Agenten. Linux Foundation, 21.5k+ GitHub Stars.

ACP
Agentic Commerce Protocol – Offener, produktiv genutzter Checkout-Standard für agentische Kaufabschlüsse (Instant Checkout). Apache 2.0 lizenziert, von OpenAI und Stripe maintained. Basis für OpenAI Instant Checkout in ChatGPT.

Agentic Commerce Alliance
Globale Industrie-Allianz für offene Standards. Gegründet Juli 2025 von Shopware unter Führung von Stefan Hamann. www.agentic-commerce.org

Agent Order
Order initiiert durch Agent mittels standardisierter Agent-Credential Headers/Token (verifizierte Agent-Identity).

Agent Surface
Oberfläche für Agent-Nutzer-Interaktion (Chat, Voice, Browser).

Agent-assisted
Agent empfiehlt, Mensch entscheidet.

Agent-executed
Agent entscheidet und handelt innerhalb Policies.

Agentic Commerce
Handel mit Agenten als delegierte Käufer.

AP2
Agent Payments Protocol – Standard für Payment Mandates und sichere, kryptographisch belegbare Agent-Zahlungsautorisierung. Google/Industry Standard.

AXP
Agentic Experience Protocol – Rich Content (3D, AR), Quality Signals, Experience Embedding. Entwickelt von Shopware und der Agentic Commerce Alliance.

Capability Ladder
5-stufiges Reifegradmodell für Agentic Commerce Readiness.

Cart Orchestration
PayPal-Service für Cart-Lifecycle-Management im Agentic Commerce.

Data Fill Rate
Vollständigkeit Produktdaten.

Digital Sales Rooms
Shopware-Feature für video-gestützte Beratung – emotionale Wertzone.

Einbettungsquote
Anteil Sessions, in denen Experience-Komponenten tatsächlich gerendert werden.

Experience Embedding
Einbettung von Rich Content (3D, AR, Konfiguratoren) in Agent-Interfaces via AXP.

Emotionale Wertzone
Bereich mit nicht-automatisierbarem Mehrwert (Sensorik, Identität, Community, Serendipität, Expertise).

Human-in-the-Loop
Menschliche Bestätigung in Prozessen.

Identity-for-Agents
PayPal-Infrastruktur für Agent-Identifikation, löst das M×N Problem.

M×N Problem
Herausforderung: M Agenten müssen mit N Händlern authentifiziert kommunizieren. Gelöst durch zentrale Identity-Provider (PayPal, Visa TAP).

MCP
Model Context Protocol – Basis-Kontexttransport. Anthropic, November 2024. Gemeinsame Integrationsschicht, unterstützt von Anthropic, OpenAI und Google.

Merchant of Record
Rechtlich verantwortliche Partei für eine Transaktion.

Policy Abort Rate
Quote der Abbrüche wegen Policy-Verletzung.

Policy File
Maschinenlesbare Regeln unter `/.well-known/agent-policy.json`.

Protokollfähig
Händler mit nativer UCP/AXP/AP2-Integration, die über standardisierte Protokolle direkt von Agenten erreichbar sind.

Quality Signals
Strukturierte Trust-Indikatoren (Reviews, Returns, Merchant Trust) via AXP.

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

Smart Wallet
Digitale Brieftasche mit Agent-Autorisierung (z. B. PayPal Smart Wallet).

Spatial Commerce
Shopware-Feature für 3D/AR-Produkterlebnisse (Apple Vision Pro, Meta Quest).

StoreSync
PayPal-Service für Product Feed Integration und Cart Orchestration im Agentic Commerce.

Trust Score
Internes KPI-Konstrukt aus Quality Signals. Externe Agenten nutzen ähnliche Signale mit eigener Gewichtung.

UCP
Universal Commerce Protocol – End-to-End-Commerce-Protokoll für Discovery, Capability Description, Order und Checkout-Orchestrierung. Google Initial Release Januar 2026, endorsed by 20+ Unternehmen.

Update Speed
Sync-Latenz zwischen Backend und Agent (Median der Sync-Zeit).

Verifiable Credentials
Kryptographisch verifizierbare Nachweise (AP2, Visa TAP).

Visa TAP
Visa Trusted Agent Protocol – Agent Identity, Consumer Recognition, Payment Information (Visa, Oktober 2025).

Weitere Ressourcen

Dieses Strategiebuch ist Teil eines umfassenden Ökosystems von Ressourcen zum Thema Agentic Commerce.

Protokoll-Portale

Weitere Protokoll-Dokumentation:

- **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

Die globale Industrie-Allianz für offene Standards. Gegründet von Shopware unter Führung von Stefan Hamann. Mitgliedschaft, Working Groups, Protokoll-Governance und Industry Events.

Expert Blog & Research

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

Stefan Hamanns persönliche Plattform mit strategischen Analysen, Deep-Dives und aktuellen Entwicklungen:

- **Whitepapers:** Technische und strategische Leitfäden zum Download
- **Industry Reports:** Analysen zu McKinsey, Morgan Stanley, IBM/NRF
- **Protocol Updates:** Neueste Entwicklungen in UCP, AXP, AP2

Technische Whitepaper

Agentic Commerce – Protocols, Standards, and Reference Architectures
Developer Technical Guide, Januar 2026, 60 min read
Umfassender technischer Leitfaden: UCP, AXP, A2A, ACP, AP2 Protokolle, Implementierungsstrategien, API-Beispiele.

Industry Reports (Primärquellen)

Quelle	Report	Kernerkenntnis
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

Tabelle 17: Industry Reports: Primärquellen für strategische Analysen.

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