digitrade

AI & Future Commerce

# When AI Agents Start Buying for Businesses, Who Decides What They Can Purchase?

AI-driven purchasing is becoming technically feasible. But buying on behalf of a business involves more than finding products and completing checkout. Before autonomous procurement can become routine, suppliers and buyers need to agree on identity, pricing, purchasing authority, and what constitutes a valid order.

A manufacturing company needs to replenish supplies for three production facilities.

Its purchasing manager asks an AI agent to review current stock requirements, identify the products due for replenishment, and prepare orders with approved suppliers.

The request sounds simple enough. Much of the information already exists in the company's systems, and software can retrieve it faster than an employee searching through several catalogs.

But suppose one product has been discontinued. A substitute is available, though it costs more and comes from a supplier the company has never purchased from.

Should the agent choose the substitute? Can it negotiate a different price? Does it have permission to use a new supplier? Who approves the additional expense?

Now suppose the agent sends a purchase order and receives no response because the connection fails. Can it safely try again without creating a duplicate?

These aren't abstract concerns about artificial intelligence. They are ordinary procurement questions that become more visible when the person performing the work is replaced, partly or entirely, by software.

**An AI agent may be able to identify what a company needs. That doesn't automatically give it the authority to buy it.**

The distinction is likely to shape the development of agentic commerce, particularly in business-to-business markets where purchasing decisions depend on contracts, budgets, approvals, and established supplier relationships.

## What changes when software becomes the buyer?

Businesses have used automated purchasing systems for decades.

An ERP can generate purchase recommendations based on inventory requirements. Procurement systems can route requisitions for approval. EDI and other electronic interfaces can transmit orders between organizations without someone manually entering every transaction.

So an AI agent placing an order isn't, by itself, a fundamentally new idea.

What changes is how purchasing decisions can be assembled and executed.

Traditional automation generally follows defined rules. When stock falls below a specified level, a system may generate a replenishment request for a known product from an approved supplier.

An AI-enabled process can potentially handle less structured instructions.

A purchasing manager might ask an agent to identify suitable alternatives, compare product documentation, investigate availability, or assemble a purchasing proposal across several suppliers.

The agent could combine information from catalogs, previous orders, contract records, and procurement policies.

Where it has appropriate tools and permissions, it could then move from preparing a recommendation to carrying out an authorized transaction.

That expands the range of tasks software can assist with. It also makes the boundary between recommendation and commitment more important.

A purchasing manager can evaluate an unfamiliar product and decide whether the risk is acceptable. Software needs explicit rules about which decisions it may make and which require human review.

The difficulty is not necessarily making an AI model produce a sensible recommendation. It is establishing that the resulting transaction satisfies the company's purchasing requirements.

## B2B purchasing involves more than a product and a payment method

Consumer-oriented discussions of agentic commerce often describe a relatively straightforward transaction.

A shopper specifies what they want, the agent finds an appropriate product, and the purchase is completed through a supported checkout process.

For many B2B transactions, important steps occur before checkout is even possible.

Consider an industrial distributor selling to a manufacturer.

The customer may have negotiated prices under an annual supply agreement. Different facilities may have different purchasing limits and delivery arrangements. Only designated employees may approve purchases above certain amounts.

Some products could be restricted to approved applications. Others may require quotations or confirmation of technical specifications.

The company may purchase on credit terms rather than paying immediately by card. An accepted order might need a valid purchase order number and an internal cost center.

None of these requirements is inherently incompatible with agent-driven purchasing.

But each must be represented somewhere in the transaction process.

An agent cannot correctly apply a customer's contract price unless the supplier can identify the account and determine which agreement is applicable.

It cannot establish that a buyer has permission to purchase without reliable authorization information.

And it should not commit a company to spending money merely because a conversational request can be interpreted as an instruction to buy.

For agentic B2B commerce to work reliably, commercial context must accompany the transaction.

## The same product may have different prices for different buyers

Imagine a supplier listing a component at $85 per unit.

One customer has negotiated a contract price of $72. Another receives a quantity discount above 500 units. A third has a project-specific quotation that expires next Friday.

An AI agent searching public product information may find the $85 price.

But that isn't necessarily the price the customer's company is entitled to pay.

Nor can the correct amount always be obtained by applying a simple customer discount.

The final price might depend on contract precedence, quantity, delivery terms, applicable promotions, or an authorized exception.

In traditional B2B ecommerce, the storefront can establish the customer's identity and request the relevant price from the supplier's commercial systems.

An external purchasing agent needs an equivalent way to establish the commercial context.

The supplier must be able to recognize the customer, determine which purchasing organization or branch is involved, identify the applicable agreement, and return an authoritative price.

If the price is provisional, that status must also be communicated.

An AI agent may be useful in comparing offers, but it should not invent commercial terms that neither party has accepted.

This becomes even more important if agents eventually negotiate.

Gartner published research in September 2026 specifically addressing the implementation of AI negotiating agents for B2B commerce. Its research abstract emphasizes the need for a defined agent experience, technology architecture, and governance controls.

The practical issue is straightforward: a seller's negotiating agent needs to know what concessions it is authorized to make. A buyer's negotiating agent needs to know what terms it may accept.

Otherwise, the two agents could reach a technically valid exchange of messages without producing an agreement either business intended to authorize.

Autonomous negotiation requires more than persuasive language. It requires enforceable commercial boundaries.

## Identity and authorization are separate problems

Suppose an agent contacts a distributor and says it represents a major manufacturing customer.

That assertion isn't sufficient.

The distributor must establish which organization the agent represents and whether the agent is authorized to act for it.

Even after the organization's identity is confirmed, additional questions remain.

Can the agent see negotiated prices for every division? Can it order for all facilities? Can it access purchasing history? What spending limit applies? Can it approve a quotation, or only prepare one?

An identity credential can help establish who—or what—is making the request. It does not automatically establish the authority attached to that identity.

That distinction is well recognized in computer security, but AI agents create additional practical challenges because they can select actions dynamically.

In February 2026, the US National Institute of Standards and Technology published a concept paper on software-agent identity and authorization. The work specifically identified authorization, auditing, accountability, and protection against prompt injection as areas requiring attention.

These are relevant concerns for any business allowing AI systems to interact with sensitive commercial records or commit transactions.

A purchasing agent should receive only the access needed for its task.

For example, an agent preparing replenishment recommendations may need permission to read inventory requirements and approved supplier catalogs. It doesn't necessarily need authority to change supplier bank details or approve an unrestricted purchase.

Similarly, an agent helping a customer place orders shouldn't gain access to negotiated prices belonging to another customer.

These controls need to be enforced by the underlying applications and APIs. A conversational instruction telling the agent to obey company policy is not an adequate substitute.

## The approval process doesn't disappear

Consider a company where purchasing authority is divided among several employees.

A maintenance manager can request equipment. A department head approves purchases above $5,000. The procurement team approves new suppliers. Finance controls certain payment commitments.

An AI agent could potentially perform much of the work required to assemble a requisition.

It might identify the requested equipment, retrieve prices, compare delivery terms, and prepare the necessary documentation.

But preparing a requisition and approving it are different actions.

The agent should not infer that an employee who can request a purchase is also allowed to authorize it.

A properly designed workflow could allow the agent to prepare the transaction, route it to the correct approver, and continue processing after approval has been recorded.

For low-value, routine purchases covered by an established policy, the business might authorize automatic approval within explicit limits.

Those decisions depend on risk, transaction value, supplier status, and the company's governance.

The important point is that human involvement should occur where the business requires a decision—not necessarily at every step of the process.

Agentic procurement doesn't have to mean purchasing without human oversight.

It can mean reducing the work surrounding decisions that still belong to people.

## Existing procurement systems already solve part of this problem

Agentic commerce is sometimes described as if businesses currently purchase everything through ordinary web stores.

That overlooks established procurement infrastructure.

Large organizations commonly use procurement applications to manage supplier catalogs, requisitions, approval processes, and purchase orders.

One established method is PunchOut.

In a typical PunchOut workflow, an employee starts in the company's procurement system and opens a supplier's catalog. The employee selects products on the supplier's website, but the selected items return to the procurement system as a requisition rather than immediately becoming a completed purchase.

The organization's approval process then determines whether a purchase order should be issued.

The cXML standard supports this interaction, along with other procurement-related documents and transactions.

That separation is significant.

The supplier may provide product information and pricing, but the buyer's organization retains control over requisition approval and the formal purchase order.

An AI agent could potentially automate parts of this workflow—for example, identifying products and preparing a requisition—without bypassing the established procurement system.

It could also interact through newer APIs, provided the required information and authorizations are available.

There is no technical reason to assume that every company will abandon existing purchasing processes simply because AI agents become more capable.

For suppliers, the relevant question is which interfaces their customers actually use and how those interfaces may evolve.

A customer that requires PunchOut or structured purchase orders today may continue requiring them while introducing AI to support the people operating its procurement process.

New agent interfaces and existing procurement protocols can therefore coexist.

## What the new commerce protocols actually provide

Recent specifications show how the infrastructure for agent-mediated purchasing is developing.

**OpenAI's Agentic Commerce Protocol (ACP) provides documented interfaces for presenting structured product information and supporting transactions through AI-mediated shopping experiences.**

Its checkout specification defines session creation, updates, completion, and order-status communication. The merchant remains responsible for authoritative pricing, validation, order acceptance, fulfillment details, and payment processing through its existing systems.

**Google's Universal Commerce Protocol (UCP) takes a broader interoperability approach. Its specification defines a way for commerce participants to advertise and consume supported capabilities, including standardized interactions between agents, applications, and businesses.**

The UCP technical documentation explicitly describes its roles in terms broad enough to include B2C, B2B, and agent-to-agent commerce.

These are meaningful developments because they introduce common interfaces for systems that might otherwise require separate integrations.

But they should not be mistaken for complete B2B procurement implementations.

A protocol can describe how a checkout session is exchanged without defining how every organization's internal spending authority is established.

It can support a way to communicate pricing without necessarily representing every negotiated contract, rebate arrangement, credit rule, or quotation workflow.

And it can facilitate a transaction without replacing the buyer's ERP, procurement policy, or approval system.

The practical distinction is between interoperability at the protocol level and completeness at the business-process level.

Both matter.

A supplier may implement an agent-facing commerce interface and still need additional work to support account-specific purchasing, contract pricing, credit terms, or customer procurement requirements.

Likewise, an existing ERP integration doesn't automatically establish compatibility with a new agentic-commerce specification.

Each layer has its own responsibilities.

## Following one purchase from request to accepted order

To see why these distinctions matter, consider a hypothetical manufacturing company purchasing replacement filters for two facilities.

Its purchasing manager asks an AI agent:

> “Replenish the standard filters for both plants. Use our existing supply agreement, avoid anything that can't arrive by Friday, and send purchases above $4,000 for approval.”

The agent retrieves the company's replenishment requirements and identifies the relevant products.

At that stage, it has established what the company may need. It has not yet established that a purchase is authorized.

Next, it contacts the approved supplier using an authorized integration.

The supplier recognizes the purchasing organization and returns the applicable products, contract prices, units of measure, availability, and delivery information.

The agent builds a proposed order for each facility.

One line item exceeds the agreed quantity limit. Another is available only after Friday.

Rather than silently changing the order, the agent identifies the exceptions.

It could recommend a compliant quantity, propose an approved substitute, or request a decision from the purchasing manager.

Suppose the corrected order for the first plant totals $3,200 and qualifies for automatic processing under the company's approved purchasing policy.

The second order totals $5,600 and requires the designated approver.

The agent can submit the first order if the buyer's system has explicitly authorized that action and the supplier's system accepts it. The second remains a proposed purchase until the required approval is recorded.

The receiving system should use a stable transaction identifier to recognize retries and prevent duplicate purchases.

The supplier's system validates the order and returns its actual acceptance state.

If the ERP rejects the transaction because of a credit restriction, the agent should report that outcome rather than claim that the purchase succeeded.

Once accepted, the supplier can provide subsequent updates about allocation, shipment, or changes to the order.

This hypothetical workflow requires several capabilities working together.

The AI needs to interpret the purchasing instruction. The buyer's systems need to enforce spending policies. The supplier needs to provide account-specific commercial data. The transaction interface needs reliable confirmation and recovery.

An agent capable of completing all those steps could substantially reduce manual coordination.

But the usefulness comes from the entire process working correctly, not merely from the AI producing a convincing purchasing recommendation.

## Payment may not happen at checkout

Another important difference between consumer and B2B commerce concerns payment.

Many consumer transactions involve an immediate card payment.

Business purchases may instead be conducted under credit arrangements, purchase orders, periodic invoicing, or other agreed terms.

A manufacturer might submit an order against an existing account and pay the invoice 30 or 60 days later, depending on its contractual agreement.

An agent supporting that transaction doesn't necessarily need to initiate a card payment.

It needs to establish that the buyer is entitled to purchase on account and that the supplier can accept the order under the applicable credit terms.

The ERP may need to validate account status, credit exposure, order limits, or outstanding restrictions.

The supplier may issue an invoice after shipment rather than collecting payment during order submission.

**Agentic commerce systems therefore need to distinguish authorizing a purchase from executing a payment.**

Those actions may occur at different times and under different controls.

Consumer-oriented payment mechanisms may be appropriate for some B2B transactions, particularly card-funded purchases.

They are not a universal substitute for commercial credit and accounts-payable processes.

Any agentic purchasing model intended for substantial B2B use must accommodate the relevant payment arrangements or integrate with systems that already do.

## What suppliers should prepare now

A manufacturer or distributor doesn't need to predict which agentic-commerce protocol will dominate in order to make useful preparations.

The most important capabilities are also valuable for conventional ecommerce.

The first is reliable, structured product information.

An agent needs consistent product identifiers, units of measure, descriptions, attributes, and other information required to identify the correct item.

Where substitutes are relevant, the supplier should distinguish verified compatibility information from informal recommendations.

The second is dependable customer-specific commercial data.

If negotiated prices, approved products, delivery locations, and customer permissions are scattered across manual records, an external agent cannot safely infer them.

Those conditions need to be represented in systems capable of producing authoritative answers.

The third is transaction-capable integration.

A supplier should be able to receive an order, validate it, return a reliable acceptance state, and communicate subsequent changes.

The interface must also handle retries, duplicate requests, failures, and exceptions.

The fourth is explicit identity and authorization.

External applications should access only the information and actions permitted to the relevant customer and purchasing role.

Finally, businesses should preserve flexibility in how those capabilities are exposed.

One buyer may continue ordering through a conventional storefront. Another may use an established procurement platform. A third may eventually use an AI agent through a standard commerce protocol.

A supplier that maintains coherent business rules and reliable APIs is better positioned to serve different channels without independently rebuilding its commercial logic for each one.

This is where ERP connectivity becomes strategically important.

If the ERP contains the authoritative customer, inventory, pricing, and order information, commerce interfaces need a dependable and appropriately governed way to use it.

The long-term opportunity is not simply to make an online store readable by an AI agent. It is to make the supplier's commercial capabilities available through authorized interfaces, regardless of whether the customer is interacting through a website, procurement application, or AI assistant.

## How quickly will autonomous procurement become common?

The direction of research and technical development is clear enough to justify attention.

In March 2026, Gartner published a research note on deploying AI agents in procurement, discussing machine buyers and how organizations might adopt them.

In August, Gartner addressed the effects of AI machine customers on supply chains. In September, it published guidance on AI negotiating agents for B2B commerce.

These publications establish that autonomous purchasing is a subject of active enterprise research and planning.

They do not establish that autonomous procurement is already widespread among US small and mid-sized businesses.

Nor does the existence of protocol specifications or working demonstrations establish how quickly customers will adopt them.

Adoption will depend on factors that extend beyond AI capability: integration costs, procurement governance, supplier participation, trust, error rates, commercial incentives, and the availability of suitable business data.

The path is also unlikely to be identical for every purchasing category.

Routine replenishment with established suppliers, stable product specifications, and clear spending rules is a plausible early application.

Complex equipment purchases, new supplier qualification, unusual technical requirements, and significant contractual negotiations may require more human involvement.

That is not a weakness of agentic commerce. It reflects differences in the underlying purchasing decisions.

Businesses should prepare for broader automation without assuming that every purchasing process will become autonomous or that every existing procurement interface will be replaced.

## The next purchasing channel still needs the same commercial foundation

Agentic commerce changes how buyers may interact with suppliers.

Instead of searching a catalog, copying product codes, requesting availability, and manually constructing an order, a purchasing professional may increasingly delegate parts of that work to software.

For suppliers, this could create new opportunities to serve customers more efficiently.

But the basic obligations of B2B selling remain.

The right customer must receive the right price. Purchasing permissions must be respected. Orders must be accepted according to agreed commercial terms. Inventory and delivery commitments must be accurate. Changes and failures must be traceable.

Those requirements do not disappear because an AI agent sits between the buyer and seller.

If anything, they become more important when transactions can proceed with less direct human intervention.

The businesses best prepared for agent-driven purchasing may therefore be those that have already made their commerce operations reliable, configurable, and connected to authoritative business systems.

An agent can make purchasing easier. It cannot compensate for commercial rules that nobody has defined or records that nobody can trust.

**The future of B2B commerce is not simply machines placing orders. It's purchasing systems that can act on behalf of businesses without losing the controls those businesses depend on.**