FICTIONAL EXAMPLE

Purchasing agent at a machine builder

Company: Huber Präzisionsteile GmbH, 180 employees, Swabia, Germany.

Situation

Purchasing orders standard parts, screws and consumables every day from about 40 suppliers. Two employees spend most of their time comparing prices and placing routine orders. An AI agent is to take this over. Management is worried that the agent will order at too high a price, too much, or from the wrong supplier.

How MolTrust is used

The purchasing agent gets its own identity (DID). The head of purchasing gives it a mandate in the AAE format: suppliers from the approved list, at most €2,000 per order, at most €15,000 per week, product group C-parts. Before every order, MolTrust checks whether the order fits this mandate. Anything outside it is blocked and passed to a member of staff.

Benefits

- Routine orders run around the clock with no manual work.
- The two employees handle supplier negotiations and shortages.
- Every order can be checked afterwards: who allowed what, and which rule applied.
- Suppliers can check for themselves that the agent is allowed to order on behalf of Huber.

> The companies in these examples are made up. The workflows show how MolTrust can be used in a mid-sized business.

Integration by IT

1. Open an account with MolTrust and register the organization.
2. Create a DID for the purchasing agent.
3. Store the rules (supplier list, limits, product groups) as a mandate, approved by the head of purchasing.
4. In the agent, add a check call to the MolTrust API before an order is sent (libraries for Node.js and Python are available).
5. Connect the check logs to the existing logging or SIEM.
6. The ERP system (for example SAP Business One or proALPHA) stays as it is; the agent orders through the existing channels.

How integration works in general

- **Effort:** Adding MolTrust takes a few minutes: get an API key, register the agent, put the check in front of the action. Step by step in the quickstart at moltrust.ch/developers.
- **Existing systems:** ERP, shop and accounting stay as they are; MolTrust is a check that runs before the agent acts.
- **Responsibility:** The business department sets the rules, IT adds the check call.
- **Data protection:** The check covers authority and action; business data stays in the company.
- **Principle:** Anything not explicitly allowed is refused.

Terms: DID (decentralized identifier, a tamper-proof digital identity for an agent). VC (verifiable credential, a digitally signed proof, for example of an authority). AAE (Agent Authorization Envelope, the MolTrust format for a mandate that sets what an agent may do). SIEM (security information and event management, central analysis of security logs).

Contact
hello@moltrust.ch · https://moltrust.ch/use-cases/einkauf/?lang=en