VELANTIA

TRUST INFRASTRUCTURE
FOR CRITICAL ACTIONS

SECTOR PACKAGE · BANKING

Providers, branches and AI agents, under provable control

Control, approval and verifiable evidence for critical actions on the bank's systems: ICT providers, internal operations, the branch network and AI agents — at the evidentiary level DORA demands.

A modern bank is operated by many hands that are not the bank's: **ICT providers intervening on the core, integrators, maintenance, growing automation and now AI agents** — while DORA requires governing and proving the resilience of all of it, third parties included. A valid credential is no longer enough as a control. *Who authorizes each intervention on your systems, under which policy, and how is it proven to the supervisor?*

WHAT VELANTIA BRINGS TO THIS SEGMENT

GATE — decides each critical action on core, payments and central systems: **allow, condition, route to approval or block** interventions by employees, providers and automations, based on policy and context.

SENTINEL — observes activity across central services and the branch network, **detects anomalies** and attributes each action to its author: employee, ICT provider, system or agent.

EVIDENCE — preserves the **evidentiary history** of every intervention and every incident: ready for internal audit, the supervisor and the incident reporting DORA requires.

AUTONOMY — governs the bank's automation and AI agents — service, operations, risk — with **explicit limits, human approval and revocation**.

WHAT YOU CAN DO WITH IT

- **Govern the ICT provider — the heart of DORA:** every third-party intervention on your systems happens under defined permissions, with an integrity-protected record of what they did.
- **Require human approval** before sensitive actions on core, payments or risk parameters — without slowing daily operations.
- **Extend control to the branch network** and channels with the same policies as central services.
- **Answer the supervisor with evidence, not narratives:** what happened, who did it, which policy applied and who approved it — already generated when the request arrives.

The bank keeps operating — every intervention with permission, context and a provable history.

DEPLOYMENT

For central services, the **CORE 900** appliance; for the branch network, **EDGE 200**; for keys and signatures, **KEY VAULT 500** with HSM and secure element from specialized partners (all in pre-order), governed from **VELANTIA ONE**. Also software, virtual machine or private cloud. It integrates with your identity, SIEM and operations **without replacing the existing stack**.

WHY NOW

DORA is already in force and the supervisor has started asking for answers: **provable resilience, governed third parties and incidents reported with evidence** — just as AI agents enter banking operations. Whoever turns compliance into real control today will face the next request with the answer already generated.

Next step: an initial meeting and a demonstration.

Complete flow on a scoped case: intervention → policy → approval or block → evidence. A scoped pilot proposal is available, with metrics and no deployment commitment.

Agustín López Mayor — Inventor · Co-founder · **Stephan Hoof** — Co-founder · International Expansion