THE MAGENTIC CONTROL FABRIC

A Standard for Dual-Intent Orchestration and Intent Zero Trust (IZT)

Author: Patrick Savio

Version: v1.0 – November 2025 (Final Publication Release)

EXECUTIVE SUMMARY

Automation executes faster than governance.
Existing Zero Trust frameworks secure identities and access - but not *purpose*.

The **Magentic Control Fabric (MCF)** introduces **Intent Zero Trust (IZT)** and **Dual-Intent Orchestration**, ensuring that every action - human or automated - is **authorized, auditable, and reversible**.

MCF operates through distributed **Model Context Protocol (MCP)** agents that communicate over authenticated A2A (Agent-to-Agent) channels under least privilege.
Each transaction follows the **Magentic Trust Loop** (Figure 1):
Intent → Validation → Execution → Observation → Audit → Accountability.

Key Contributions

1. Dual-Intent Architecture: unifies human and automation intent under shared policy.
2. Intent Zero Trust (IZT): extends "never trust, always verify" to *purpose itself*.
3. Three Governance Laws:
    1. No automation without intent.
    2. No intent without audit.
    3. Every audit must enable accountability.
4. Defensive Back Shield: compliance engine aligned with EU AI Act [1], NIST AI RMF [2], OECD [3], ISO/IEC 42001 [4].
5. Verified Identity & RACI Mapping: enforces oversight, cryptographic attribution, and accountability.

Outcome:
MCF converts regulation into executable control logic - automation that acts fast *and* legitimately.

A. ABSTRACT

The Magentic Control Fabric (MCF) formalizes **Dual-Intent Orchestration** and **Intent Zero Trust (IZT)** - a security plane where *purpose* becomes the object of trust.
It operationalizes ethics and compliance, enabling trustworthy automation at scale for enterprises and SMBs.

B. EXECUTIVE FOREWORD - THE INTENT-BOUND FUTURE

Automation has outpaced accountability.
MCF restores purpose as the organizing principle of automation, merging **human intent** (purpose, boundaries) and **automation intent** (conditions, triggers) under explicit policy.

The Three Laws of Magentic Governance
1 - No automation without intent.
2 - No intent without audit.
3 - Every audit must enable accountability.

C. DEFINITIONS AND TERMINOLOGY

Term	Definition
Intent	Verifiable expression of purpose and authorization describing why an action should occur.
Human Intent	Originates from a verified human actor; carries ethical accountability.
Automation Intent	Triggered by system conditions or policy; carries operational justification.
Dual-Intent System	Requires both human and automation intents for authorization.
Model Context Protocol (MCP)	Open protocol for model↔tool interaction; each MCP is a role-scoped agent in authenticated A2A trust.
Intent Manifest	Signed document defining origin, scope, policy, creation and expiry timestamps.
Intent Gate	Policy-driven checkpoint validating or denying intents.
Back Shield	Compliance and risk parser evaluating bias, fairness, rights, and risk confidence.
Audit Ledger	Immutable record of intent decisions and outcomes.

Reversibility	Restores state via snapshots and journals within a defined window.
Trust Boundary	Any perimeter across which intents must be revalidated.

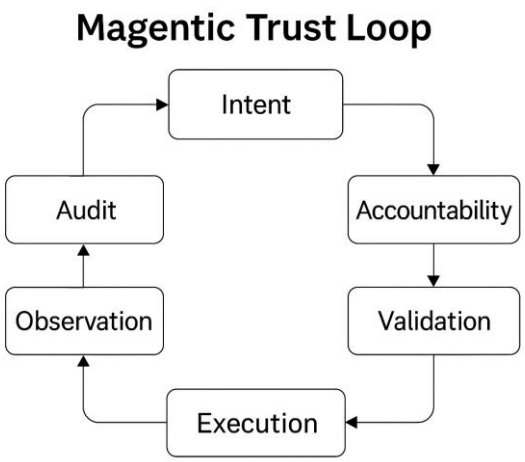
D. DESIGN DOCTRINE - THE THREE LAWS AND THE MAGENTIC TRUST LOOP

Law 1: No Automation Without Intent
Every autonomous action must originate from a declared intent.

Law 2: No Intent Without Audit
Every intent must produce an immutable record.

Law 3: Every Audit Must Enable Accountability
Audit provides observation; accountability enforces governance and reversibility.

Figure 1 - The Magentic Trust Loop



E. ARCHITECTURAL OVERVIEW

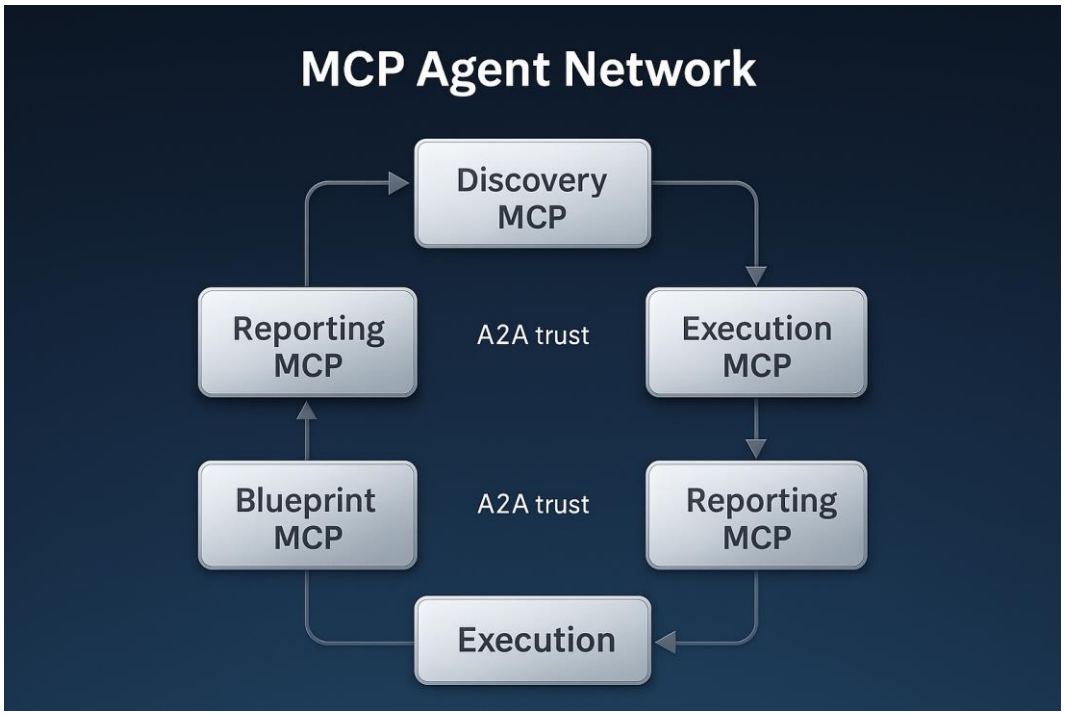
E.1 Planes of Operation

1. Intent Plane: origin of human and automation intents.
2. Validation Plane: Back Shield and Orchestrator MCP evaluate intent legitimacy.
3. Orchestration Plane: MCP agents execute authorized actions under least privilege.
4. Evidence Plane: Audit Ledger and Accountability systems record outcomes.

E.2 MCP Agent Roles and Resilience

MCP Agent	Function	Privilege Scope
Discovery MCP	Scans telemetry and context.	Read-only
Blueprint MCP	Maps policies and execution plans.	Read / derive
Execution MCP	Executes authorized actions and requests re-authorization if scope changes.	Controlled write
Reporting MCP	Aggregates logs into Audit Ledger.	Read-only
Orchestrator MCP	Routes and validates intents under policy consensus using cryptographic token rotation and quorum-based validation to avoid single-point compromise.	Delegated trust

Figure 2 - MCP Agent Network



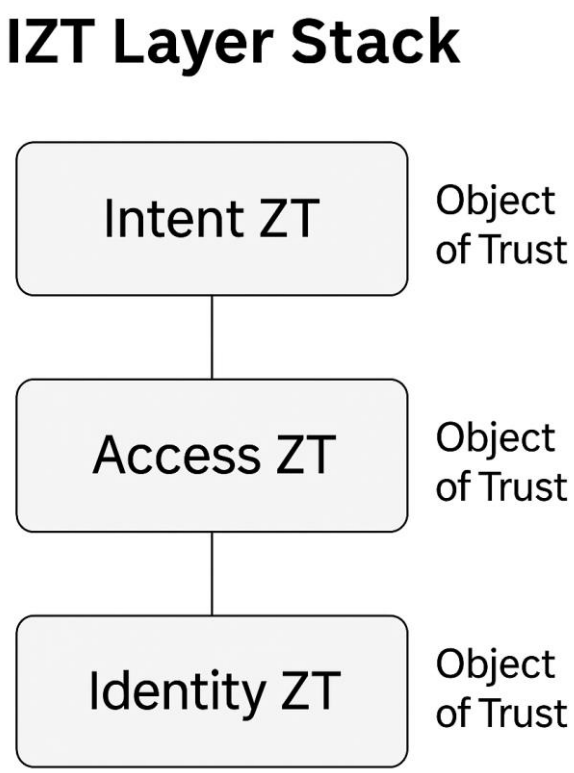
F. INTENT ZERO TRUST (IZT)

IZT extends Zero Trust to purpose itself.
No intent is trusted by default; each must prove origin, policy, privilege, and reversibility.

Layer	Core Question	Object of Trust
Intent ZT	Why are you acting?	Purpose
Access ZT	What can you reach?	Resource
Identity ZT	Who are you?	Credential

IZT applies recursively in multi-agent systems where nested intents require hierarchical validation.

Figure 3 - IZT Layer Stack



G. ARCHITECTURE OF TRUST - RUNTIME OPERATION

1. Intent submitted (human or automation).
2. Back Shield evaluates risk, fairness, rights.
3. Orchestrator authorizes (automatic or step-up).
4. Execution MCP acts under least privilege.
5. Reporting MCP and Audit Ledger capture records.
6. Accountability feedback forms a new intent cycle.

H. REVERSIBILITY MECHANISMS

1. State Snapshots: restore system state before critical changes.
2. Transaction Journals: record intent mutations with rollback keys.
3. Time-Bound Reversal Window: locks after verified external impact.

I. GOVERNANCE AND ETHICS

“No irreversible change may occur without traceable human authorization.”
Automation codifies human boundaries. Ambiguous context triggers verification pause.

J. COMPLIANCE AND CONFORMANCE

A system is *Magentic-Compliant* when it:

– Implements Dual-Intent Orchestration through Intent Gates.
– Applies IZT verification to all actions.
– Maintains an immutable Audit Ledger.
– Provides reversibility and human override for critical actions.

K. ANNEX A - REGULATORY CONFORMANCE FRAMEWORK

A.1 Purpose

Aligns MCF with EU AI Act [2], NIST RMF [2], OECD [3], ISO [4], eIDAS [9].

A.2 Defensive Back Shield

Metric	Threshold
Bias Index	≤ 5 %
Risk Confidence	≥ 95 %
Rights Impact Flag	= 0

Model-agnostic; integrates via API hooks with AI/ML frameworks.

A.3 Risk-Driven Authorization and Oversight

Risk Class	Action	Human Oversight	Regulatory Source
Low	Normal flow	Automated approval	NIST RMF §MAP
Limited	Contextual review	Periodic check	AI Act Art 9
High	Step-up auth	Real-time approval	AI Act Art 14
Unacceptable	Blocked	Incident record	AI Act Art 5

A.4 Dynamic Red-Teaming and SAST

Continuous testing and secure code scanning; pipelines halt on failure (ISO/IEC 27035 [10]).

A.5 Ethical Training and Data Integrity

Bias audit, provenance validation, model hashing, training-time Back Shield validation.

A.6 Verified Human Identity

Actors verified via trusted credentials (eIDAS 2.0 [9]).

A.7 RACI Accountability Mapping

Role	Responsible	Accountable	Consulted	Informed
Discovery MCP	Telemetry	Orchestrator MCP	Compliance	Board
Blueprint MCP	Policy Mapping	Orchestrator MCP	Legal	Board
Execution MCP	Authorized Actions	Ops Lead	Security	Reporting
Reporting MCP	Audit Aggregation	Compliance Officer	DPO	Stakeholders
Orchestrator MCP	Intent Validation	Executive	Compliance	All
Back Shield	Risk Analysis	Compliance Officer	Regulators	Board

A.8 Verified Oversight and Non-Repudiation

Step-up events cryptographically signed; records immutable and identity-bound.

A.9 Regulatory Mapping Summary

Objective	MCF Mechanism	Regulation
Risk Assessment	Back Shield	AI Act Art 9
Fairness & Rights	Back Shield Parser	OECD P2
Human Oversight	Step-Up Auth	AI Act Art 14
Robustness	Red-Teaming + SAST	ISO 27035
Training Integrity	Bias Audit + Hash	ISO 42001
Identity & Accountability	Verified ID + RACI	eIDAS 2.0
Transparency	Logs & Ledger	AI Act Art 12
Documentation	Ledger Records	NIST RMF
Ethics	Validation Before Execution	OECD P1

L. GLOSSARY APPENDIX

Back Shield: Validation layer for risk, fairness, rights.
Dual-Intent Orchestration: Joint human and automation authorization.
Intent Zero Trust (IZT): Verification of purpose as a trust object.
MCP: Model Context Protocol agent framework.
Magentic: Multi agentic
Reversibility: Controlled state restoration and rollback.
RACI: Responsible, Accountable, Consulted, Informed governance matrix.

REFERENCES

[1] NIST AI Risk Management Framework (2023)
[2] EU Artificial Intelligence Act (Final Text, 2024)
[3] OECD Principles on AI (2019)
[4] ISO/IEC 42001 AI Management System (2023)
[5] Microsoft Zero Trust Maturity Model (2021)
[6] IBM AI Ethics Guidelines (2022)
[7] OpenAI Model Governance Protocols (2024)
[8] 5G Americas Intent-Based Automation Frameworks (2023)

[9] European Commission eIDAS 2.0 Regulation (2024)
[10] ISO/IEC 27001 & 27035 Information Security Standards (2022)

Formal Citation

Savio, P. (2025). The Magentic Control Fabric - A Standard for Dual-Intent Orchestration and Intent Zero Trust (IZT). Version 1.0, November 2025. Licensed under CC BY-SA 4.0.