

# SAP Joule and Enterprise AI Agent Interoperability Architecture

A Comprehensive Enterprise Architecture for Secure, Governed, and Standards-Based Interoperability Between SAP Joule, AI Agents, Business Applications, Data, and Tools

Sanjeeve Kumar Gajadi\*

\*(HCL Technologies, Bengaluru, Karnataka, India)

Email: [sanjeevekumar.g@hcltech.com](mailto:sanjeevekumar.g@hcltech.com)

\*\*\*\*\*

## Abstract:

Enterprises are increasingly adopting SAP Joule alongside custom AI agents, third-party copilots, orchestration platforms, business applications, and data services. Without a common interoperability architecture, these components can create duplicated capabilities, inconsistent context, weak identity propagation, fragmented tool access, and governance gaps. This paper proposes a SAP Joule and Enterprise AI Agent Interoperability Architecture that defines interaction patterns across SAP and non-SAP systems. The architecture addresses agent identity, delegated authorization, semantic context, business APIs, events, SAP BTP services, SAP Integration Suite, SAP Business Data Cloud, tool registries, orchestration, observability, and policy enforcement. It introduces interoperability layers for user experience, agent coordination, context and knowledge, business capabilities, integration, security, governance, and monitoring. The proposed approach enables organizations to combine SAP Joule with enterprise AI agents while preserving business semantics, authorization boundaries, auditability, reuse, and platform independence.

**Keywords** — SAP Joule, Agentic AI, SAP BTP, AI Interoperability, SAP Integration Suite, SAP Business Data Cloud, AI Agents, Enterprise Architecture, AI Governance, Business APIs

\*\*\*\*\*

## I. INTRODUCTION

SAP Joule can provide conversational and AI-assisted experiences across SAP business processes, while enterprises may also deploy custom or third-party AI agents.

Interoperability architecture is required so that these agents exchange context and invoke business capabilities without bypassing SAP security, semantics, or governance.

## II. ARCHITECTURE PRINCIPLES

Principles include business capability reuse, identity continuity, least privilege, semantic consistency, API-first integration, event awareness, policy enforcement, and observable agent behavior.

The architecture should avoid point-to-point agent connections that create hidden dependencies and uncontrolled tool access.

## III. EXPERIENCE AND INTERACTION LAYER

Users may interact through SAP Joule, enterprise portals, mobile applications, collaboration tools, or specialized agents.

Conversation context should be scoped and transferred only when required for the receiving agent or business task.

## IV. AGENT COORDINATION LAYER

Coordination services should manage delegation, routing, task ownership, capability discovery, and conflict resolution across agents.

Each delegation should preserve the identity and authority chain and record the purpose of the task.

## V. BUSINESS CAPABILITY AND TOOL LAYER

SAP and non-SAP business functions should be exposed as governed tools or APIs with explicit schemas, authorization, validation, and audit requirements.

Reusable tool contracts reduce duplication and allow Joule and other agents to invoke the same approved business capabilities.

## VI. SAP BTP AND INTEGRATION LAYER

SAP BTP can provide integration, extension, workflow, security, data, and application services supporting agent interoperability.

SAP Integration Suite can mediate APIs, events, transformations, and connectivity between SAP and non-SAP systems.

## VII. DATA AND KNOWLEDGE LAYER

SAP Business Data Cloud, SAP Datasphere, governed data products, and enterprise knowledge sources can provide contextual information for AI interactions.

Retrieval should preserve data ownership, semantics, lineage, and user or agent entitlements.

## VIII. IDENTITY AND AUTHORIZATION

Human, agent, application, and tool identities should remain distinguishable throughout the interaction chain.

Delegated authorization should limit access by purpose, scope, time, business object, and transaction risk.

## IX. SEMANTIC INTEROPERABILITY

Business object definitions, capability models, metadata, and semantic contracts should reduce ambiguity between SAP and non-SAP agents.

Semantic consistency is essential when agents exchange customer, product, order, finance, service, or workforce information.

## X. GOVERNANCE AND POLICY ENFORCEMENT

Policies should govern which agents can collaborate, which tools they may invoke, what data they may access, and when human approval is required.

Governance decisions should be enforced at runtime rather than relying only on design-time documentation.

## XI. OBSERVABILITY AND AUDITABILITY

End-to-end traces should capture agent routing, prompts, retrieved context, SAP and non-SAP tool calls, authorization decisions, approvals, and business outcomes.

Shared correlation identifiers allow investigations to follow a task across Joule, custom agents, integration services, and backend systems.

## XII. IMPLEMENTATION ROADMAP

Organizations can start with a small set of reusable business capabilities and clearly defined Joule-to-agent interaction patterns.

Later stages can add multi-agent orchestration, shared knowledge, event-driven coordination, dynamic capability discovery, and automated governance.

## XIII. CONCLUSION

The SAP Joule and Enterprise AI Agent Interoperability Architecture enables enterprises to combine SAP-native and external AI capabilities without fragmenting control.

By standardizing identity, business interfaces, semantics, integration, and observability, organizations can scale agentic AI while maintaining enterprise governance and SAP process integrity.

## ACKNOWLEDGMENT

The author acknowledges the contributions of enterprise architecture practitioners, AI governance specialists, security professionals, standards bodies, and technology researchers whose published work informed the concepts synthesized in this paper.

## REFERENCES

- [1] National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), 2023.
- [2] National Institute of Standards and Technology, AI RMF Generative Artificial Intelligence Profile, 2024.
- [3] ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system.
- [4] ISO 31000:2018, Risk management — Guidelines.
- [5] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — Information security management systems.
- [6] National Institute of Standards and Technology, SP 800-207: Zero Trust Architecture, 2020.
- [7] The Open Group, TOGAF Standard, 10th Edition, 2022.
- [8] ISACA, COBIT 2019 Framework: Governance and Management Objectives, 2019.

- [9] OWASP Foundation, OWASP Top 10 for Large Language Model Applications.
- [10] MITRE, ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems.
- [11] OECD, Recommendation of the Council on Artificial Intelligence.
- [12] IEEE, Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems.