International Journal of Technology Management & Humanities (IJTMH)
e-ISSN: 2454 – 566X, Volume 6, Issue 3-4, (July-December 2020), www.ijtmh.com

A Federated Identity-Centric Architecture for Secure Hybrid SAP Integration and Zero-Trust Enterprise API Management

Rakesh Mallik
Department of Computer Science, Indraprastha University, New Delhi, India
rakesh_malikdsciu@yahoo.co.in

Abstract

Hybrid SAP landscapes connect on-premise SAP ECC systems with cloud platforms, SaaS applications, and partner services through a growing number of APIs. In these environments, identity rather than network location has become the most reliable basis for trust, yet many organizations still manage identities, credentials, and interface permissions separately in each system. This paper proposes a federated identity-centric architecture in which a verified identity context is created once, carried through every integration hop, and evaluated by zero-trust policies at each API boundary. The architecture comprises five planes: a federated identity plane, a token and trust brokering plane, a zero-trust API management plane, a data protection plane, and an observability and adaptive response plane. It draws on research into hybrid SAP integration security (Asuri, 2019), risk-centric threat detection across SAP landscapes (Asuri, 2020), and hybrid cloud data placement (Sannidhanam & Alladi, 2017), together with established work on delegated authorization (Hardt, 2012), perimeter-free enterprise access (Ward & Beyer, 2014), federation assurance (Grassi et al., 2017), and zero trust architecture (Rose et al., 2020). The paper describes the architecture, traces three representative integration scenarios through it, and evaluates it qualitatively against security and interoperability objectives. The result is a practical blueprint for SAP architects who need to open business processes to cloud and partner consumers without weakening accountability or control.

Keywords: Federated identity, hybrid SAP integration, SAP ECC, zero trust, API management, OAuth 2.0, SAML 2.0, principal propagation, SIEM, data protection

1. Introduction

For many enterprises, SAP ECC remains the system of record for finance, procurement, logistics, and human resources. At the same time, new business capabilities are increasingly delivered through cloud services, SaaS applications, mobile channels, and partner ecosystems. The result is a hybrid landscape in which business transactions routinely cross from on-premise systems to cloud platforms and back again, often passing through middleware, cloud connectors, and API gateways along the way.

Each of these crossings is a trust decision. Traditionally, SAP security relied on two foundations: a protected corporate network and the SAP authorization concept applied to named users inside the system. Hybrid integration erodes both. Cloud consumers sit outside the corporate network, and integration traffic frequently runs under shared technical users whose broad authorizations

bear no relation to the person who started the transaction. When something goes wrong, audit logs show only that a technical account performed an action, not who requested it or why.

Asuri (2019) identifies fragmented identity administration, inconsistent access policies, insufficient interface protection, and inadequate monitoring as the principal risks of hybrid SAP integration. These risks share a common root: identity is treated as a local concern of each system rather than as an enterprise-wide asset that travels with every request. When identity is fragmented, every other control, from API authorization to audit logging, inherits that weakness.

This paper takes the opposite position. It argues that a secure hybrid SAP landscape should be designed around identity first, with the API layer acting as the point where identity is verified and policy is enforced. Zero trust, which grants no implicit trust based on network location (Rose et al., 2020), provides the governing principle. Federation standards provide the mechanism for carrying identity across organizational and technical boundaries (Grassi et al., 2017).

The paper makes three contributions. First, it synthesizes the relevant literature on hybrid SAP security, threat detection, data placement, delegated authorization, and zero trust. Second, it proposes a five-plane, identity-centric reference architecture for hybrid SAP integration. Third, it traces representative integration scenarios through the architecture and evaluates it against defined design objectives.

2. Literature Review

2.1 Security of hybrid SAP integration

Asuri (2019) studies identity federation, API authorization, and data protection between SAP ECC and SAP Cloud Platform using a mixed-method design of architectural analysis, control assessment, and comparative evaluation of established practices. The study proposes a layered model combining federated identity, role-based access control, secure API gateways, encrypted transmission, and centralized audit. Its key insight is that identity assurance, interface security, and information protection must be designed as one architecture. The present paper adopts that insight and places identity explicitly at the centre of the design.

2.2 Risk-centric threat detection in SAP landscapes

Asuri (2020) proposes a methodology for detecting cyber threats across SAP landscapes using security event correlation, statistical anomaly profiling, and enterprise-wide SIEM analytics. The work matters here because an identity-centric architecture creates rich, attributable telemetry. When every request carries a verified identity, events from the identity provider, the API gateway, and SAP audit logs can be joined into coherent user-level activity trails, making correlation and anomaly profiling far more effective.

2.3 Hybrid placement of sensitive data

Sannidhanam and Alladi (2017) describe a hybrid cloud storage architecture for large-scale medical data in which data is classified, highly confidential and frequently accessed records are kept in a private environment, and archival or less sensitive data is placed in public cloud. Encryption, access control, synchronization, and disaster recovery support the design. Although

the domain is healthcare, the principle that placement and protection should follow data classification applies directly to SAP business data exposed through hybrid integration.

2.4 Delegated authorization and federation standards

Hardt (2012) specifies the OAuth 2.0 authorization framework, which allows a client application to obtain limited, scoped access to a protected resource on behalf of a resource owner through access tokens issued by an authorization server. OAuth 2.0 separates the roles of client, resource server, and authorization server, which makes it well suited to API-based integration. Grassi et al. (2017), in NIST SP 800-63C, define federation assurance levels and describe how identity providers and relying parties establish trust, protect assertions, and bind them to subscribers. Together, these documents provide the technical and assurance vocabulary for carrying identity across hybrid boundaries.

2.5 Zero trust architecture

Ward and Beyer (2014) describe Google's BeyondCorp initiative, which removed the privileged corporate network and based access decisions on authenticated users and managed devices. Their account shows that perimeter-free access can work at enterprise scale. Rose et al. (2020), in NIST SP 800-207, formalize zero trust architecture around a policy engine, a policy administrator, and policy enforcement points that evaluate each access request dynamically using identity, device posture, and contextual signals. This model maps naturally onto an API gateway acting as the enforcement point for SAP interfaces.

2.6 Research gap

The SAP-specific studies establish the risks and control categories of hybrid integration, while the standards literature supplies general models for federation and zero trust. What is missing is an architecture that applies these general models specifically to SAP integration patterns, including principal propagation into ECC, mapping of tokens to SAP authorizations, and correlation of identity and SAP audit data. This paper addresses that gap.

3. Research Method

The study uses a design-oriented approach consistent with the mixed-method orientation of Asuri (2019). It proceeds in four steps. First, the seven sources were reviewed to extract design principles, threats, and control categories. Second, five design objectives were defined from that review: end-to-end identity continuity, least-privilege access, explicit verification of every request, data protection proportionate to classification, and full attributability of actions. Third, a reference architecture was constructed to satisfy those objectives. Fourth, three representative integration scenarios were traced through the architecture, and the design was evaluated qualitatively against each objective. The architecture has not been implemented or measured empirically in this study.

4. Proposed Architecture

The architecture is organized into five planes. Each plane has a distinct responsibility, but all of them share a single identity context that is established once and preserved end to end.

4.1 Federated identity plane

The identity plane establishes who or what is making a request.

- **Authoritative identity provider.** A corporate identity provider (IdP) authenticates employees, while partner identity providers are federated through explicit trust relationships rather than local partner accounts.
- **Federation protocols.** SAML 2.0 supports browser-based single sign-on to SAP cloud applications, while OAuth 2.0 supports delegated API access (Hardt, 2012).
- **Assurance levels.** Each federation relationship is assigned an assurance level appropriate to the data and transactions involved, following the federation assurance concepts of Grassi et al. (2017).
- **Workload identities.** Technical integrations receive their own registered identities with narrowly scoped credentials instead of shared technical users.
- **Lifecycle governance.** Joiner, mover, and leaver events from the HR system drive provisioning and deprovisioning across ECC, cloud subaccounts, and partner trust lists.

4.2 Token and trust brokering plane

The brokering plane translates identity between the protocols spoken by different systems.

- **Token exchange.** A central authorization server issues short-lived access tokens and exchanges tokens when a request moves from one trust domain to another.
- **Principal propagation.** When a cloud service calls ECC through a connector, the end user's identity is propagated so that ECC evaluates the user's own SAP authorizations, not those of a generic technical user.
- **Scope-to-role mapping.** OAuth scopes are mapped to SAP business roles through a maintained catalogue, so that a cloud scope such as "read supplier invoices" corresponds to a defined set of ECC authorizations.
- **Certificate and key management.** Signing keys and certificates used for assertions, tokens, and mutual TLS are rotated centrally.

4.3 Zero-trust API management plane

The API management plane is where policy is enforced. In the terms of Rose et al. (2020), the API gateway acts as the policy enforcement point, while a policy engine evaluates each request.

- **Single front door.** All APIs that cross the hybrid boundary are published through the gateway; direct point-to-point exposure of ECC services is not permitted.
- **Per-request evaluation.** Each call is checked for a valid token, required scopes, client identity, and contextual conditions such as time, location, and request rate.
- **API product catalogue.** Every API is registered with an owner, a data classification, permitted consumers, and a version lifecycle, making exposure visible and reviewable.
- **Payload controls.** Schema validation, size limits, and field-level filtering reduce injection risk and prevent bulk extraction.

- **Interoperability.** Because consumers integrate against governed, documented APIs rather than system-specific interfaces, new cloud and partner applications can be onboarded consistently.

4.4 Data protection plane

The data protection plane applies controls according to data classification, following the tiered approach of Sannidhanam and Alladi (2017).

- Business data is classified by sensitivity and regulatory relevance.
- Highly sensitive records remain in ECC or controlled private environments; replication to cloud services is limited to what a business process requires.
- Data is encrypted in transit and at rest, with keys under enterprise control.
- APIs return only the fields that a consumer's scope permits, and sensitive fields are masked where full values are unnecessary.
- Backup and recovery arrangements cover replicated data, not only the system of record.

4.5 Observability and adaptive response plane

The final plane closes the zero-trust loop by feeding observed behaviour back into access decisions, building on Asuri (2020).

- Identity provider logs, token issuance records, gateway telemetry, SAP security audit logs, and cloud audit logs are collected in an enterprise SIEM.
- Because every event carries the same propagated identity, events can be correlated into user-level and workload-level activity trails.
- Statistical baselines of normal behaviour identify anomalies such as unusual data volumes, new consumer locations, or off-hours access.
- Risk scores feed the policy engine, which can require step-up authentication, shorten token lifetimes, revoke tokens, or block an API consumer.

5. Representative Integration Scenarios

5.1 Employee using a cloud application backed by ECC

An employee signs in to a cloud procurement application through SAML single sign-on at the corporate IdP. The application requests an OAuth token to call an ECC purchase order API. The gateway validates the token and scopes, and the connector propagates the employee's identity to ECC, which applies the employee's own authorizations. The SIEM records a single, attributable trail from sign-in to transaction.

5.2 Partner system submitting invoices

A supplier's system authenticates through its own identity provider, federated with the enterprise at a defined assurance level. The authorization server issues a token limited to an invoice submission scope. The gateway enforces schema validation and rate limits, and the data protection plane ensures the partner can see only its own documents. Any deviation from the partner's normal submission pattern raises an alert.

5.3 Machine-to-machine replication to analytics

A scheduled integration replicates selected financial data from ECC to a cloud analytics service. It runs under a registered workload identity with read-only scopes for specific data sets. Fields classified as highly sensitive are masked before leaving the on-premise environment, and any request outside the approved schedule or volume is blocked and investigated.

6. Evaluation Against Design Objectives

Design objective	How the architecture addresses it
End-to-end identity continuity	Federation, token exchange, and principal propagation preserve the original identity across every hop
Least-privilege access	Scoped tokens, workload identities, and scope-to-role mapping limit each consumer to what it needs
Explicit verification	The gateway evaluates every request against current policy and context
Proportionate data protection	Classification drives placement, encryption, field filtering, and masking
Full attributability	Correlated logs link each action to a verified person or workload

The evaluation is qualitative. It shows that each objective is supported by at least two planes, which reduces dependence on any single control. It also shows that interoperability improves alongside security, because standard protocols and a governed API catalogue replace system-specific integration methods.

7. Discussion

7.1 Implications for practice

The architecture reframes SAP integration security as an identity problem. For SAP architects, this means that decisions about connectors, middleware, and API exposure should start with the question of how identity will be carried and verified. For security teams, it means that SAP audit data becomes far more valuable once it can be joined with identity and gateway telemetry, as anticipated by Asuri (2020). For the business, a governed API catalogue shortens the time needed to connect new cloud and partner services safely.

7.2 Implementation challenges

Several challenges should be expected. Older ECC interfaces such as RFC and IDoc may not support token-based authentication natively and may need to be mediated through middleware or the gateway. Mapping cloud scopes to SAP roles requires careful collaboration between business owners and SAP security teams and is best done incrementally, starting with the highest-risk processes. Principal propagation depends on consistent user identifiers across systems, which may require identity data cleanup. Finally, per-request policy evaluation adds latency, so policies should be tuned to the sensitivity of each API.

7.3 Limitations

This study is conceptual. The architecture has not been deployed or measured, and its evaluation relies on reasoning against design objectives rather than empirical data. The literature base is small, and the transfer of hybrid data placement principles from healthcare to SAP is argued by analogy. These limitations define the agenda for future work.

8. Conclusion

Hybrid SAP landscapes cannot rely on network boundaries or shared technical users to establish trust. This paper proposed a federated identity-centric architecture in which identity is established once, propagated through every integration hop, and verified under zero-trust policy at each API boundary. Five planes, covering identity, token brokering, API management, data protection, and observability, work together to deliver continuity of identity, least privilege, explicit verification, proportionate data protection, and full attributability. Grounded in SAP-specific research and established federation and zero-trust standards, the architecture offers a practical path for organizations that need to extend SAP business processes to cloud and partner consumers securely. Future research should validate it through pilot implementations, measure its effect on incident detection and integration effort, and develop maturity models for phased adoption.

References

Asuri, R. (2019). Strengthening hybrid SAP enterprise integration through federated identity assurance, zero-trust API governance, and resilient data protection across SAP ECC and cloud environments. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 11*(02), 191–208. https://smsjournals.com/index.php/SAMRIDDHI/article/view/3584

Asuri, R. (2020). A risk-centric methodology for detecting cyber threats across SAP landscapes using security event correlation, statistical anomaly profiling, and enterprise-wide SIEM analytics. *International Journal of Technology, Management and Humanities, 6*(01–02), 1–25. https://doi.org/10.21590/ijtmh.06.1-2.03

Grassi, P. A., Richer, J. P., Squire, S. K., Fenton, J. L., Nadeau, E. M., Lefkovitz, N. B., Danker, J. M., Choong, Y.-Y., Greene, K. K., & Theofanos, M. F. (2017). *Digital identity guidelines: Federation and assertions* (NIST Special Publication 800-63C). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-63c

Hardt, D. (Ed.). (2012). *The OAuth 2.0 authorization framework* (RFC 6749). Internet Engineering Task Force. https://doi.org/10.17487/RFC6749

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sannidhanam, A. H., & Alladi, S. (2017). A hybrid cloud storage architecture for large-scale medical data. *International Journal of Food Safety and Public Health, 4*(1), 01–09. https://ijpp.org/journal/index.php/ajb/article/view/585

Ward, R., & Beyer, B. (2014). BeyondCorp: A new approach to enterprise security. *;login: The USENIX Magazine, 39*(6), 6–11.