iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

HYBRID CONNECTIVITY ARCHITECTURE FOR SAP RISE DEPLOYMENTS:

DESIGN PATTERNS FOR SECURE CLOUD CONNECTOR INTEGRATION WITH SAP BUSINESS TECHNOLOGY PLATFORM AND THIRD-PARTY BOUNDARY SYSTEMS

Srinivas Kakarla
SAP Architect
SAP RISE · Hybrid Integration · SAP Business Technology Platform (BTP) · SAP Cloud Connector

Abstract
The RISE with SAP programme, launched by SAP SE in January 2021, fundamentally redefines the enterprise SAP deployment model by shifting infrastructure management to SAP while preserving the customer's business processes in a managed private cloud. While RISE with SAP dramatically simplifies the infrastructure operational burden, it introduces a new and complex challenge: maintaining secure, reliable, and observable hybrid connectivity between the SAP-managed cloud environment, the enterprise's remaining on-premises SAP and non-SAP systems, the SAP Business Technology Platform (BTP) integration middleware, and an expanding ecosystem of third-party SaaS and partner boundary systems. The SAP Cloud Connector (SCC) is the primary enabler of this hybrid connectivity, establishing outbound-initiated tunnels from the on-premises network to BTP that eliminate the need for inbound firewall rules - yet the SCC's architecture, high-availability configuration, security hardening requirements, and operational monitoring are frequently under-specified in enterprise SAP programmes.
This article presents a comprehensive set of validated design patterns for hybrid connectivity in SAP RISE deployments. Drawing on authoritative SAP, Microsoft, and hyperscaler documentation available through October 2022, the article addresses four primary connectivity scenarios: on-premises-to-BTP via SAP Cloud Connector, RISE-to-hyperscaler private network via Private Link Service, third-party API integration via BTP API Management, and identity federation across boundary systems via SAP Identity Authentication Service. For each scenario, the article provides architecture diagrams, security design principles, operational runbook guidance, and anti-pattern analysis. The validated design patterns are synthesised into a reference architecture suitable for enterprise SAP programmes embarking on the RISE migration journey.

Keywords:
SAP RISE; SAP Cloud Connector; BTP Connectivity Service; Hybrid Integration; Private Link; OAuth 2.0; SAP IAS; ExpressRoute; API Gateway; Zero Trust; SAP Integration Suite; Network Security

1. Introduction

Enterprise SAP landscapes have historically been defined by their complexity: multiple ERP instances, spanning decades of customisation, integrated through thousands of RFC connections, BAPIs, IDocs, and file-based interfaces into a web of interdependencies that makes change management one of the most demanding disciplines in enterprise IT. The RISE with SAP programme represents the most significant structural change to this landscape in two decades. By contracting SAP SE as the managed cloud infrastructure provider for the core ERP system, organisations accelerate their path to SAP S/4HANA while transferring significant infrastructure operational responsibility. Yet the promise of simplification is conditional: the ERP core may move to a managed cloud, but the integration landscape that surrounds it does not disappear overnight.
Hybrid connectivity - the secure, reliable exchange of business data between the SAP RISE managed environment, on-premises systems, BTP integration services, and third-party platforms - is the architectural discipline that makes the RISE deployment viable for complex enterprise landscapes. At the centre of this discipline is the SAP Cloud Connector (SCC), a lightweight Java-based agent installed on-premises that establishes an outbound TLS tunnel to the SAP BTP Connectivity Service. This architecture avoids the need to open inbound firewall ports for

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

SAP BTP-initiated calls to on-premises systems - a security property that is architecturally elegant but operationally demanding to configure and maintain at enterprise scale.

Beyond the SCC, the full connectivity architecture for a RISE deployment in a large enterprise encompasses hyperscaler private networking (Azure Private Link or AWS PrivateLink), API management gateways for third-party integrations, identity federation chains that span corporate Active Directory, SAP IAS, and partner identity providers, and an operational monitoring layer that provides end-to-end observability across all of these components. The design of this connectivity architecture is not addressed in detail in SAP's RISE marketing materials; it is a technical architecture challenge that each enterprise must solve with reference to SAP's documentation, hyperscaler architectural guidance, and field experience from the growing but still limited body of completed RISE deployments as of 2022.

This article addresses that gap. The design patterns presented here are derived from SAP's official documentation, BTP product team publications, hyperscaler architectural guidance from Microsoft and AWS, and the emerging academic and practitioner literature on SAP cloud integration patterns available through October 2022. The article is structured around four primary connectivity scenarios - on-premises-to-BTP, RISE-to-hyperscaler, third-party API integration, and identity federation - each treated as a discrete, composable design pattern that can be combined to form the full hybrid connectivity architecture.

> **Scope Note:** *This article focuses on the SAP RISE with SAP deployment model on hyperscaler infrastructure (Azure and AWS). RISE on SAP-owned data centres (Dedicated Tenancy) has distinct network architecture constraints not covered here. All connectivity patterns described are compatible with SAP S/4HANA Cloud Private Edition (formerly PCE) as of the November 2022 publication date.*

2. SAP RISE Architecture: Connectivity Foundations

Figure 1 — High-Level Hybrid Connectivity Architecture Overview

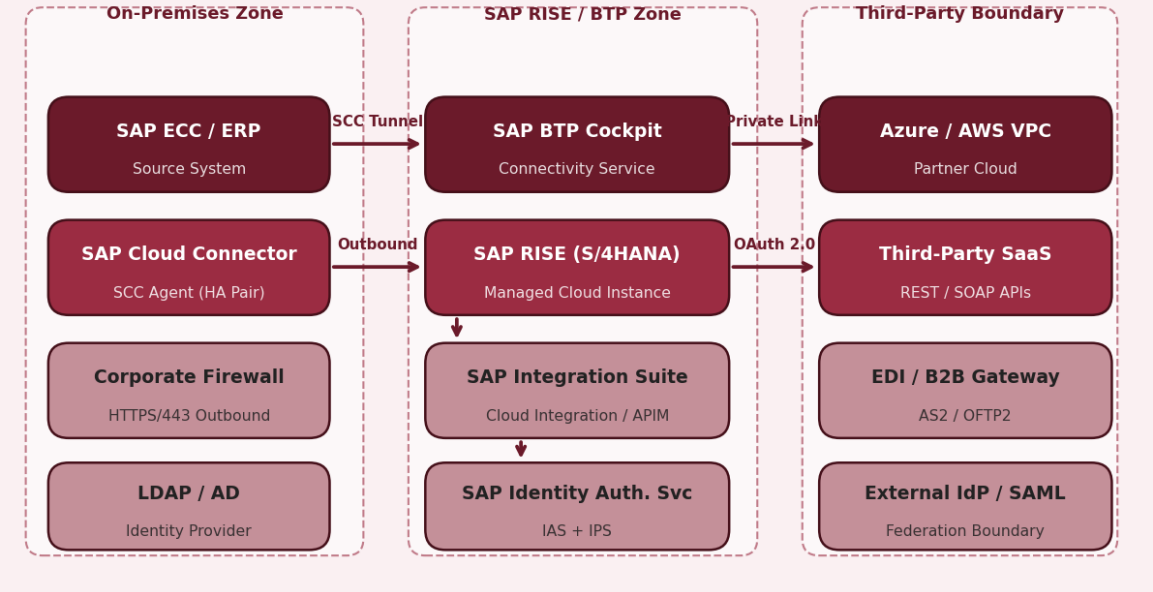

Figure 1 - High-Level Hybrid Connectivity Architecture Overview

2.1 RISE with SAP Deployment Model

RISE with SAP bundles the SAP S/4HANA Cloud Private Edition license, managed cloud infrastructure (provided by either SAP directly or a hyperscaler partner), SAP Business Technology Platform entitlements (Integration Suite, Extension Suite, Analytics Cloud), and SAP cloud services (SAP Signavio Process Intelligence,

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

SAP Business Network Starter Pack) into a unified subscription offering. The critical architectural implication for connectivity is that the S/4HANA system is deployed in a virtual network segment managed by SAP - customers do not have direct VPN or peering access to the S/4HANA VM network by default.

Connectivity to the RISE-managed S/4HANA system from the enterprise network is enabled through three primary mechanisms:

- SAP Cloud Connector tunnel: For RFC, HTTP, and JDBC connections from on-premises systems to S/4HANA or BTP services, initiated outbound from the corporate network.
- Private Link Service: For private, hyperscaler-managed network connectivity between the enterprise's own Azure VNet or AWS VPC and the SAP-managed cloud network, without traversing the public internet.
- SAP BTP Integration Suite: For event-driven, API-based, and message-based integration flows orchestrated by the BTP integration middleware layer, which acts as a neutral integration broker between all connectivity zones.
- SAP Web Dispatcher: For HTTPS-based user access to SAP Fiori, SAP Web GUI, and ABAP ODATA services, typically fronted by an enterprise load balancer or Application Delivery Controller in a DMZ.

2.2 Connectivity Responsibilities Under RISE

A frequently misunderstood dimension of RISE with SAP is the shared responsibility model for connectivity. SAP is responsible for the managed S/4HANA infrastructure, its internal network security, and the SAP-side configuration of connectivity services. The customer retains responsibility for on-premises SCC deployment and configuration, corporate firewall rules allowing SCC outbound traffic, custom BTP subaccount configuration, third-party API credentials and certificates, and the end-to-end monitoring of integration flows. The boundary between SAP-managed and customer-managed components varies depending on the RISE contract type and hyperscaler choice.

- **SAP-Managed:** S/4HANA virtual machines, HANA database, OS patching, SAP kernel updates, hyperscaler infrastructure, internal S/4HANA network, SAP BTP platform infrastructure.
- **Customer-Managed:** SAP Cloud Connector installation and HA configuration, corporate network routing and firewall policy, BTP subaccount setup, destination service configuration, third-party integration certificates and credentials, monitoring and alerting for custom integration flows.
- **Jointly Managed:** Private Link configuration (customer creates service endpoint; SAP approves connection), identity provider trust configuration (customer configures IAS federation; SAP BTP uses IAS), SAP Integration Suite iFlow development and deployment (customer builds; BTP runs).

> **Architecture Insight:** *The RISE shared responsibility boundary is not a hard technical line - it is a contractual and operational delineation. Effective hybrid connectivity architecture requires the enterprise architecture team to map every connectivity component explicitly to either the SAP-managed or customer-managed domain and to define clear operational handoff procedures at the boundary.*

3. SAP Cloud Connector: Architecture and High Availability

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

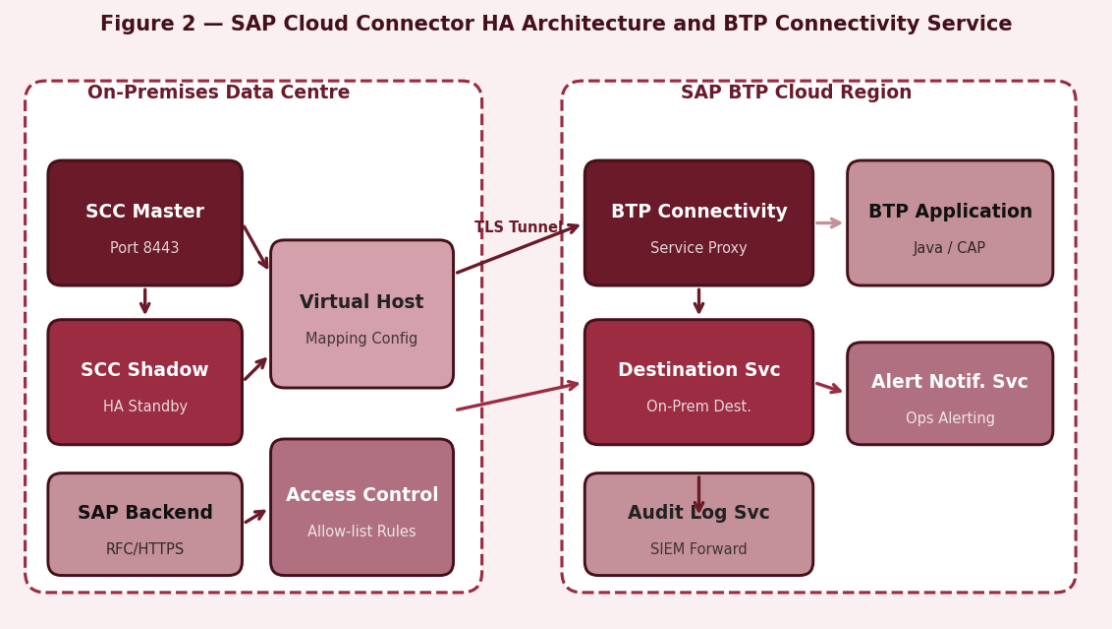

Figure 2 - SAP Cloud Connector HA Architecture and BTP Connectivity Service

3.1 SCC Tunnel Mechanism and Security Model

The SAP Cloud Connector establishes a persistent, mutually authenticated TLS tunnel from the on-premises host to the SAP BTP Connectivity Service. This design is deliberately asymmetric: the tunnel is always initiated by the SCC (outbound from the corporate network), never by BTP. This eliminates the requirement to open any inbound firewall ports for SAP BTP, which would be prohibited by most enterprise network security policies. The tunnel uses TLS 1.2 or TLS 1.3 over HTTPS (port 443) and is authenticated using X.509 certificates exchanged during the initial SCC-to-BTP account pairing.

The fundamental security properties of the SCC tunnel mechanism are as follows:

- Outbound-only initiation: Corporate firewalls need only permit outbound TCP/443 from the SCC host to BTP's Connectivity Service endpoint - no inbound rules are required, dramatically reducing the network attack surface.
- Mutual TLS authentication: Both the SCC agent and the BTP Connectivity Service authenticate using X.509 certificates, preventing unauthorised endpoints from establishing tunnels to either side.
- Virtual host mapping: On-premises SAP systems are not directly exposed to BTP; instead, the SCC maps internal hostnames and ports to virtual host aliases that BTP applications use. The actual backend hostname is never transmitted over the tunnel, providing a layer of obscurity for internal network topology.
- Access control lists: The SCC administrator configures explicit allow-lists specifying which BTP subaccounts, which virtual hosts, and which URL paths are accessible through the tunnel. Deny-by-default access control prevents accidental exposure of internal resources.
- Audit logging: All connection attempts through the SCC - both successful and rejected - are logged with subaccount, timestamp, source IP, destination virtual host, and URL path, providing a complete audit trail for security operations.

3.2 High-Availability SCC Deployment Patterns

The SAP Cloud Connector supports a master-shadow high availability configuration in which a secondary SCC instance (shadow) monitors the primary (master) and automatically takes over tunnel maintenance if the master becomes unavailable. The shadow SCC synchronises configuration from the master at regular intervals and maintains its own outbound connection to BTP, enabling near-instantaneous failover without requiring BTP-side

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

configuration changes. Failover is transparent to BTP applications and on-premises backends - the virtual host mappings and access control lists remain unchanged.

- Master-Shadow topology: The master SCC handles all active tunnel traffic; the shadow SCC maintains a hot standby state, synchronising configuration changes from the master via a dedicated HA communication channel on configurable port (default: 8444).
- Physical separation: Master and shadow SCC instances must reside on separate physical or virtual hosts to provide fault domain isolation. Deploying both on the same physical host negates the HA benefit - a host failure would take both instances offline simultaneously.
- Shared configuration storage: SCC configuration (subaccount connections, virtual host mappings, access control rules, certificate bindings) is stored in a local file system on each SCC host; the shadow synchronises this state from the master. Backup procedures must cover both hosts.
- Monitoring and alerting: The BTP Connectivity Service exposes an API for programmatic SCC connection health monitoring; this API should be polled by the operations monitoring system and alerts raised within 60 seconds of SCC disconnection to meet typical RTO requirements for integration availability.
- Certificate rotation procedures: SCC instance certificates expire and must be rotated without disrupting active tunnels. The rotation procedure differs depending on whether the SCC uses its own self-signed certificate or an enterprise PKI-issued certificate, and must be rehearsed in non-production environments before production execution.

3.3 SCC Security Hardening

The default SCC installation provides a functional but not fully hardened configuration. Enterprise security standards require additional hardening steps that are documented in SAP's SCC Administration Guide but frequently overlooked in project timelines. The following security hardening requirements are non-negotiable for production RISE deployments:

- Replace the default self-signed SCC instance certificate with a certificate issued by the enterprise PKI or a trusted commercial CA, to enable certificate chain validation by BTP and to align with enterprise certificate governance policies.
- Configure TLS version restrictions to disable TLS 1.0 and TLS 1.1 on the SCC administration UI (port 8443) and on the tunnel interface, allowing only TLS 1.2 and TLS 1.3.
- Enable SCC logon screen security to prevent username enumeration through error message differentiation - the SCC should return identical error messages for invalid usernames and incorrect passwords.
- Restrict SCC administration UI access by configuring IP-based access controls to limit the administration interface to the enterprise's IT operations network segment only.
- Integrate SCC audit logs with the enterprise SIEM platform (Splunk, Azure Sentinel, IBM QRadar) using syslog forwarding or the SAP Audit Log Service, ensuring real-time correlation of SCC access events with identity and network security events.
- Configure the SCC host OS firewall to block all inbound connections except port 8443 (administration) from approved management subnets and the SCC HA communication port from the shadow instance host.

4. Design Pattern 1 - On-Premises to BTP via Cloud Connector

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

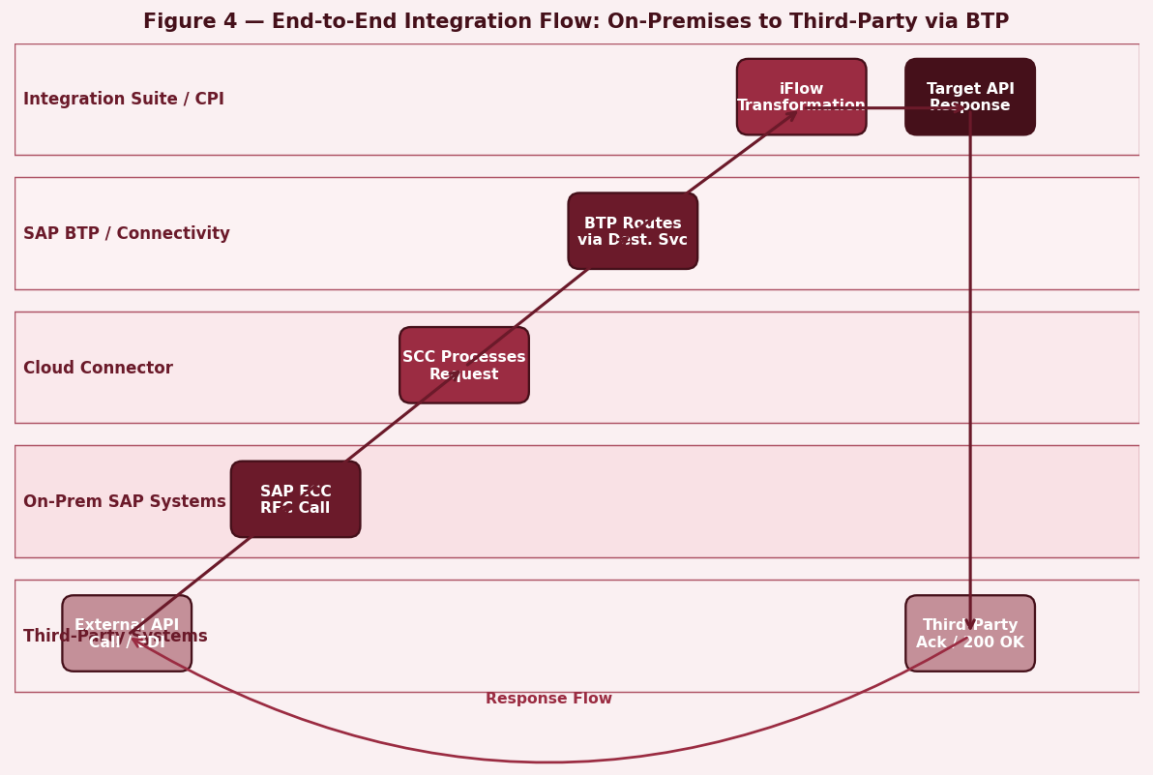

Figure 4 - End-to-End Integration Flow: On-Premises to Third-Party via BTP

4.1 Connectivity Service and Destination Service Integration

The BTP Connectivity Service acts as the cloud-side termination point for the SCC tunnel. When a BTP application (running in Cloud Foundry, Kyma, or a standalone service) needs to call an on-premises system, it does not call the on-premises system directly; instead, it calls the Connectivity Service proxy, which routes the request through the appropriate SCC tunnel to the virtual host that maps to the target on-premises backend. This transparent proxying means BTP application code does not contain any on-premises network topology information - only virtual hostnames configured by the SCC administrator.

The BTP Destination Service complements the Connectivity Service by providing a centralised store for connection configurations (endpoints, authentication credentials, certificate references) that BTP applications retrieve at runtime. Destinations can be defined at the BTP subaccount level (shared across all applications in the subaccount) or at the individual application level. Destination configurations include an on-premise flag that instructs the runtime to route the outbound call through the Connectivity Service proxy and the SCC tunnel.

- Destination types for on-premises connectivity include HTTP destinations (for ABAP ODATA services, SAP Fiori, and REST APIs), RFC destinations (for SAP RFC function modules and BAPIs), LDAP destinations (for on-premises Active Directory lookups), and MAIL destinations (for SMTP relay through corporate mail servers).
- Authentication options for on-premises destinations include Basic Authentication (username/password stored as encrypted destination properties), Principal Propagation (forwarding the cloud user's identity to the on-premises system through header-based identity propagation configured in the SCC), Client Certificate (mutual TLS with P12/PFX key store referenced in the destination), and OAuth2 Client Credentials (for modern SAP services that accept OAuth tokens).
- Principal Propagation is the recommended authentication approach for RISE deployments where the on-premises system must enforce user-level authorisation: the cloud user's identity (from IAS) is propagated

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

through the SCC to the ABAP system, where standard SAP authorisation objects control access. This eliminates the need for shared service account credentials in on-premises systems.

- Destination cloning between BTP subaccounts (development, quality, production) must be managed carefully: credentials and endpoints differ between landscapes, and destination configuration must be part of the landscape-specific provisioning pipeline, not manually copied.

4.2 Access Control and Virtual Host Mapping

The SCC's access control mechanism is the primary technical safeguard preventing unauthorised access to on-premises systems from BTP. Every resource accessible through the SCC tunnel must be explicitly declared in the SCC access control configuration - there is no wildcard or default-allow capability. The access control entry specifies the virtual host name, the protocol (HTTP, HTTPS, RFC, LDAP), and the URL path or RFC function module pattern that is permitted. Any BTP request for a resource not in the allow-list is rejected by the SCC before it reaches the on-premises network.

- Virtual host naming convention: Adopt a consistent virtual host naming scheme (e.g., <system-id>-<client>.<landscape>.corp.internal) that encodes system identity and landscape level, enabling SCC administrators to identify the target system from the virtual hostname alone without referencing external documentation.
- Minimum-privilege access control: Each SCC access control entry should permit only the specific URL paths or RFC function groups required by the BTP application. Avoid path wildcards (/*) unless the BTP application genuinely requires broad access - a misconfigured wildcard entry is the most common SCC security finding in penetration tests.
- Access control review cadence: SCC access control entries should be reviewed quarterly and upon any change to the connected BTP application portfolio. Entries for decommissioned BTP applications must be actively removed - the SCC does not automatically prune stale entries when a BTP subaccount is deleted.
- RFC function module allow-listing: For RFC destinations, the access control entry specifies a function module name pattern (e.g., BAPI_SALESORDER_* or Z_CFIN_*). Restrict RFC access to specific BAPI families and custom function modules required by the integration, not the entire RFC function catalogue.

5. Design Pattern 2 - RISE to Hyperscaler via Private Link

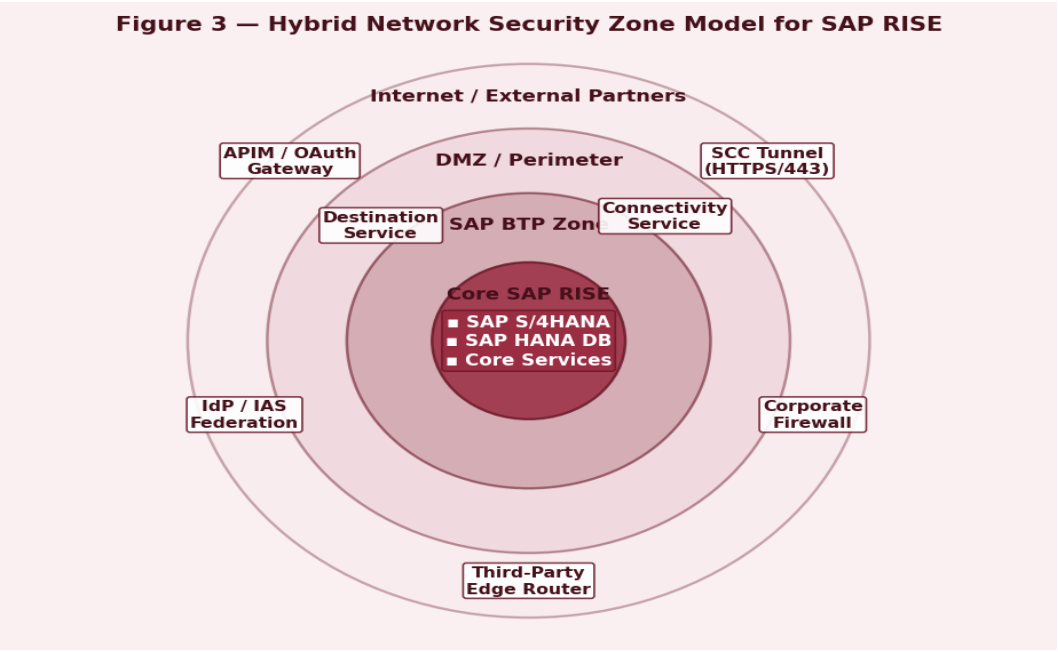

Figure 3 - Hybrid Network Security Zone Model for SAP RISE

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

5.1 Azure Private Link / AWS PrivateLink Integration

Private Link Service (Azure) and AWS PrivateLink provide hyperscaler-native mechanisms for establishing private, non-internet-routed network connectivity between the SAP RISE managed VNet and the enterprise's own cloud VNet. Unlike the SCC tunnel - which operates at the application layer and is suitable for individual service calls - Private Link operates at the network layer, providing a persistent private IP endpoint in the enterprise VNet that resolves directly to services running in the SAP-managed network segment. Private Link is the preferred connectivity mechanism for high-throughput, low-latency use cases such as HANA database access from enterprise analytics tools, SAP Landscape Transformation (SLT) replication traffic, and bulk RFC-based data migration workloads.

The Private Link architecture for SAP RISE involves the following components and design decisions:

- SAP Private Link Service (BTP service): SAP has published a dedicated BTP Private Link Service that abstracts the hyperscaler-specific Private Link configuration, allowing BTP applications to consume on-enterprise-side endpoints through Private Link without managing the underlying Azure or AWS constructs directly.
- Azure Private Link Service (on enterprise side): The enterprise creates a Private Link Service fronted by an Azure Standard Internal Load Balancer that exposes the target service (e.g., an enterprise API gateway, a legacy system adapter) to the SAP RISE VNet through a private endpoint.
- DNS resolution: Private Link endpoints use private IP addresses that are not publicly resolvable. Azure Private DNS Zones or Route 53 Private Hosted Zones must be configured to resolve the SAP-provided service hostname to the private endpoint IP within the enterprise VNet, without leaking resolution to the public DNS hierarchy.
- Network policy implications: Private Link bypasses Network Security Groups by default in Azure - explicit NSG policies on the subnet hosting the private endpoint must be configured to enforce traffic filtering. This is a commonly misconfigured aspect of Private Link deployments that can result in unintended broad network access.
- Approval workflow: Private Link connection requests from the SAP side must be approved by the enterprise network team before the connection becomes active. This approval step should be integrated into the SAP RISE onboarding change management process, with a maximum 24-hour SLA for approvals to avoid blocking project milestones.

5.2 Network Routing and DNS Resolution

Correct DNS resolution is the most operationally sensitive aspect of Private Link deployments for SAP. Because SAP RISE S/4HANA and BTP services use hostnames that resolve to public IP addresses in normal DNS resolution, but must resolve to private endpoint IPs within the enterprise network, the enterprise DNS infrastructure must implement split-horizon DNS - returning private IP answers to internal resolvers and public IP answers to external resolvers for the same hostnames.

- Implement Azure Private DNS Zones linked to all VNets that need to resolve SAP Private Link endpoints, with A records pointing to the private endpoint IP addresses. Ensure that on-premises DNS servers have conditional forwarders configured to use Azure DNS for the SAP-specific domain zones.
- Validate DNS resolution from every network zone before go-live: from on-premises domain-joined workstations, from BTP Cloud Foundry application containers, from Kyma pods, and from Azure-hosted integration VM servers. DNS misconfiguration is the most common cause of connectivity failures in the initial RISE go-live phase.
- Establish a DNS change management process for SAP RISE-related DNS records: as SAP updates or rotates the Private Link endpoint configuration, the enterprise DNS records must be updated in synchronisation. This operational dependency should be documented in the RISE connectivity runbook.
- Avoid hairpin routing through the internet for any SAP connectivity path that can be served through Private Link or the SCC tunnel. Internet egress for SAP traffic introduces unpredictable latency, exposes internal

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

hostname patterns in DNS queries visible to public DNS resolvers, and creates a security boundary that is harder to monitor than private network paths.

6. Design Pattern 3 - Third-Party API Integration via BTP APIM

6.1 API Management as Boundary Gateway

SAP API Management (part of BTP Integration Suite) serves as the policy enforcement boundary for API-based integrations between the RISE S/4HANA environment and third-party systems. In hybrid connectivity terms, APIM acts as an outbound gateway for S/4HANA-initiated API calls to external services (partner B2B APIs, logistics providers, banking APIs) and as an inbound gateway for third-party-initiated calls into the SAP landscape (webhook callbacks, EDI acknowledgements, real-time data feeds). Centralising all third-party API traffic through APIM provides a single point of control for authentication enforcement, rate limiting, payload transformation, error handling, and audit logging.

- Inbound policy enforcement: All APIs published through APIM should have an OAuth 2.0 or API key authentication policy applied as a mandatory inbound policy. Unauthenticated API endpoints should not exist in a production APIM instance - every endpoint must require a valid credential.
- Rate limiting and quota policies: Apply rate limiting policies (requests per second) and quota policies (requests per day) to all third-party-facing API endpoints to prevent abuse and protect the underlying SAP systems from being overwhelmed by runaway integration clients.
- Payload validation: Configure APIM to validate inbound JSON or XML payloads against published API schemas before forwarding requests to the BTP backend. Schema validation at the API gateway layer prevents malformed payloads from reaching SAP Integration Suite iFlows or ABAP function modules.
- API versioning strategy: Adopt a URL-based API versioning scheme (/api/v1/, /api/v2/) from the outset of the APIM configuration, enabling non-breaking version transitions when SAP or business requirements drive API contract changes that would otherwise break third-party integrations.
- Developer portal and API discovery: Publish a developer portal through APIM for third-party integration partners, providing API documentation, sandbox endpoints, and self-service credential provisioning. Reducing the manual coordination burden on the SAP integration team significantly accelerates third-party onboarding timelines.

6.2 OAuth 2.0 and Token-Based Security Patterns

OAuth 2.0 is the recommended authentication framework for all REST API integrations between BTP services, SAP RISE S/4HANA, and third-party systems. BTP provides a built-in OAuth 2.0 Authorization Server through the SAP Authorization and Trust Management Service (XSUAA), which issues access tokens for BTP service instance access. For third-party integrations, the appropriate OAuth 2.0 grant type depends on the integration scenario:

- OAuth 2.0 Client Credentials Grant: Used for machine-to-machine integrations where no user identity is involved - for example, a third-party logistics system posting shipment status updates to S/4HANA. The third-party system authenticates using a client ID and secret to obtain an access token from XSUAA, then uses the token for API calls.
- OAuth 2.0 JWT Bearer Grant: Used when the calling system holds a JWT assertion (from a trusted IdP) that can be exchanged for a BTP-specific access token. Preferred for integrations where the calling system is also an OAuth 2.0-capable cloud service (Salesforce, Workday, ServiceNow) that issues its own JWTs.
- OAuth 2.0 SAML Bearer Assertion Grant: Used for principal propagation scenarios where the end user's SAML assertion from the enterprise IdP is exchanged for a BTP XSUAA access token. Enables user-context-aware API calls from on-premises systems through BTP, maintaining the audit trail of user identity throughout the integration chain.
- Token caching and refresh strategy: OAuth access tokens issued by XSUAA have a configurable expiry (typically 12 hours). Integration clients should implement token caching to avoid requesting new tokens

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

for every API call, and should implement silent refresh (using a refresh token or re-executing the client credentials flow) before token expiry to prevent integration failures during long-running background jobs.

- Client secret rotation: OAuth 2.0 client secrets stored in BTP service instance bindings and in third-party system credential stores must be rotated according to the enterprise security policy (typically 90-day maximum). Establish a documented rotation procedure that updates the secret simultaneously in both the BTP XSUAA service binding and the third-party integration client configuration to avoid a rotation-induced outage.

7. Design Pattern 4 - Identity Federation Across Boundaries

7.1 SAP IAS as Central Identity Broker

SAP Identity Authentication Service (IAS) is the recommended identity broker for SAP RISE deployments, providing a single point of identity federation between the corporate identity infrastructure (Active Directory, Azure AD, Okta) and all SAP applications in the RISE landscape. IAS supports SAML 2.0 and OpenID Connect protocols on both its service-provider (consuming identity from upstream IdPs) and identity-provider (providing identity to downstream SAP applications) interfaces, enabling flexible topology configurations.

The IAS-centric identity architecture provides the following capabilities that are particularly valuable in a hybrid RISE deployment:

- Identity lifecycle management: IAS IPS (Identity Provisioning Service) synchronises user accounts from the corporate HR system (SuccessFactors or on-premises HR) to all SAP cloud applications in the RISE landscape, ensuring user provisioning and de-provisioning are executed within the SLA required by access governance policies.
- Corporate IdP proxy: IAS acts as a proxy between the corporate Identity Provider (e.g., Azure AD with MFA enforcement) and SAP applications. Users authenticate to the corporate IdP; IAS receives the SAML assertion, enriches it with SAP-specific attributes (SAPuser, cost centre, role assignments), and forwards an enriched assertion to the target SAP application.
- Risk-based authentication: IAS supports conditional authentication rules that elevate authentication requirements based on risk signals (unfamiliar device, unusual geographic location, access to sensitive resources). These rules complement and extend the corporate IdP's Conditional Access policies specifically for SAP application access.
- Multiple corporate IdP support: Large enterprise groups with multiple acquired subsidiaries often have multiple Active Directory forests and identity providers. IAS can federate with up to 50 corporate IdPs simultaneously, presenting a single unified identity endpoint to all SAP applications in the RISE landscape.

7.2 Corporate IdP Integration and Trust Configuration

Establishing the trust configuration between the corporate IdP, IAS, and individual SAP applications requires careful coordination of SAML metadata exchange, attribute mapping, and certificate management across multiple systems. The following design decisions govern IAS trust configuration in RISE deployments:

- Trust topology: Configure the corporate IdP as an upstream Identity Provider in IAS (IAS acts as SP toward the corporate IdP), and configure IAS as the Identity Provider for BTP subaccounts and SAP applications (BTP/apps act as SPs toward IAS). This creates a clean two-hop federation chain: Corporate IdP → IAS → SAP Application.
- NameID format alignment: Ensure consistent NameID formats across the federation chain. Microsoft Azure AD issues NameIDs in email address format by default; SAP ABAP systems may require numeric user IDs. IAS attribute mapping rules must transform the NameID to the format expected by each SAP application.
- Certificate rotation plan: IAS SAML signing certificates expire (typically every 2–5 years) and must be rotated by updating the SAML metadata exported from IAS and importing it into both the upstream corporate IdP and all downstream SAP application SPs. This multi-system coordination is a significant operational event that should be rehearsed and documented before production certificate expiry.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- Emergency access: Design an emergency access path that bypasses the corporate IdP federation chain - for example, local IAS administrator accounts or SAP system emergency (firefighter) accounts - to enable SAP access when the corporate IdP is unavailable. This emergency path must be protected by its own MFA mechanism (IAS TOTP or hardware key) and subject to the same audit logging as normal access.
- Third-party IdP integration for partner access: When third-party organisations (auditors, implementation partners, BPO providers) require direct access to the RISE S/4HANA system, configure a dedicated corporate IdP connection in IAS for the third-party's identity provider rather than issuing local IAS accounts. This ensures third-party access is governed by the third-party's own identity lifecycle management processes.

8. Security Architecture for Hybrid Connectivity

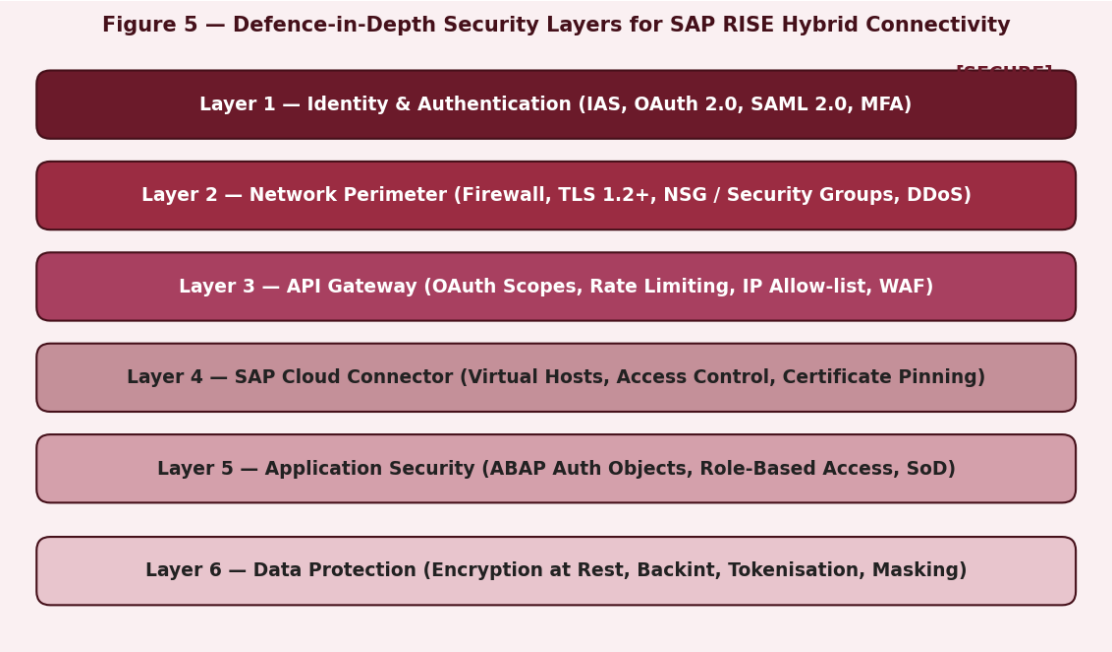

Figure 5 - Defence-in-Depth Security Layers for SAP RISE Hybrid Connectivity

8.1 Defence-in-Depth Controls

The security architecture for SAP RISE hybrid connectivity is structured as six concentric layers, each providing independent security controls that collectively implement a defence-in-depth posture. No single layer is sufficient on its own; the strength of the architecture derives from the combination of controls across all layers. Each layer addresses a distinct attack surface and threat model.

- Layer 1 - Identity and Authentication: IAS with corporate IdP federation, OAuth 2.0 client credentials for M2M flows, MFA enforced for all human access, Just-in-Time user provisioning via IAS IPS, emergency access governance via SAP GRC Emergency Access Management.
- Layer 2 - Network Perimeter: SCC outbound-only tunnel (no inbound firewall rules), TLS 1.2/1.3 minimum for all transit encryption, Private Link for direct network connectivity (no internet routing), DDoS protection on public endpoints, enterprise firewall policy for SCC host egress.
- Layer 3 - API Gateway: APIM OAuth 2.0 policy enforcement on all endpoints, payload schema validation, rate limiting and quota enforcement, IP allow-listing for trusted partner subnets, WAF rules for OWASP Top 10 protection on BTP-exposed APIs.
- Layer 4 - SAP Cloud Connector: Virtual host mapping (obscures internal topology), access control allow-lists (deny by default), audit logging of all tunnel traffic, certificate-based SCC instance authentication, TLS inspection by enterprise firewall of SCC egress traffic.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- Layer 5 - Application Security: SAP ABAP authorisation objects and roles, SoD conflict detection via SAP GRC Access Control, principal propagation preserving user identity through the integration chain, custom ABAP code security review against SAP Code Vulnerability Analyser (CVA) findings.
- Layer 6 - Data Protection: Encryption at rest for all SAP data (HANA DVE and hyperscaler disk encryption), TLS for all data in transit, tokenisation of sensitive fields in integration payloads where regulatory requirements mandate it, GDPR-compliant data residency enforcement through BTP region selection and Private Link geographic constraints.

8.2 Certificate Management and Rotation

Certificate management is one of the highest-risk operational areas in hybrid SAP connectivity. Certificate expiry events that are not proactively managed cause sudden connectivity failures that manifest as integration blackouts - often during critical business periods when the failed integration was last tested and verified to be working. The certificate landscape in a RISE hybrid connectivity deployment includes:

- SCC instance certificate: Authenticates the SCC to BTP Connectivity Service. Expiry causes immediate tunnel disconnection. Must be monitored with minimum 60-day renewal lead time. Rotation procedure: generate new key pair, request certificate from enterprise PKI, update SCC instance certificate configuration, verify tunnel re-establishment.
- BTP destination client certificates: Used for client certificate authentication on HTTP and RFC destinations. Stored in BTP Destination Service certificate stores. Must be rotated before expiry and the rotation coordinated with the on-premises system's trusted certificate store update.
- IAS SAML signing certificate: Signs SAML assertions issued by IAS to SAP applications. Expiry causes SSO failures across all IAS-federated applications simultaneously. Rotation requires SAML metadata re-exchange with all connected SPs and IdPs - a multi-system coordination event with a minimum 2-week execution window.
- Corporate IdP SAML certificate: Expires according to the corporate IdP's certificate rotation policy (typically 1–3 years). IAS must be updated with the new IdP metadata before the old certificate expires. Calendar reminders should be set 90 days before expiry across the enterprise architecture, SAP Basis, and identity management teams.
- TLS certificates for Custom Domains: BTP custom domain certificates for externally-facing SAP Fiori and API endpoints follow standard web PKI certificate lifecycles (1-year maximum per CA/B Forum requirements from 2020). Automate renewal using Let's Encrypt ACME protocol or enterprise CA automation wherever possible.

> **Certificate Management Insight:** *Implement a certificate inventory with expiry tracking across all connectivity components as a Day 1 operational requirement - not a post-go-live improvement. A centralised certificate register updated as part of every connectivity configuration change eliminates the "we didn't know it was expiring" incident pattern that is responsible for a disproportionate share of SAP RISE connectivity outages.*

9. Operational Monitoring and Observability

Observability for SAP RISE hybrid connectivity requires a multi-layer monitoring strategy because the connectivity chain spans multiple administrative domains, multiple technology stacks, and multiple vendor-managed platforms. A failure in an integration flow can originate from any point in the chain - the on-premises backend system, the SCC tunnel, the BTP Connectivity Service, the BTP Integration Suite iFlow, the APIM gateway, the RISE S/4HANA system, or the third-party endpoint - and the monitoring architecture must provide sufficient instrumentation to localise the failure within 5 minutes for P1 integration incidents.

- SCC connectivity monitoring: Monitor the BTP Connectivity Service health API for SCC connection status at 30-second intervals. Set a P1 alert if any production SCC subaccount connection reports disconnected status for more than 60 seconds. Include the SCC master-shadow failover event as a P2 alert with a 5-minute response SLA.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- BTP Integration Suite monitoring: Configure iFlow execution monitoring in BTP Integration Suite to alert on: error message rate exceeding 5% of daily average, any message stuck in "processing" status for more than 10 minutes, and backlog queue depth exceeding 1,000 messages. Route all alerts to the operations ITSM platform.
- End-to-end transaction tracing: Implement correlation IDs in integration flows that propagate the originating transaction ID from the source system through the BTP iFlow to the S/4HANA posting and to any third-party callbacks. This enables end-to-end trace reconstruction for failed transactions using the BTP Message Monitor and S/4HANA Application Log.
- API Management analytics: APIM provides built-in analytics dashboards for request volume, error rates, response times, and top consumers per API endpoint. Set alert thresholds for API error rates exceeding 1% on production endpoints and for response times exceeding the SLA defined in partner integration agreements.
- Identity and authentication monitoring: Monitor IAS authentication success and failure rates, SAML assertion issuance volumes, and any spike in failed authentication attempts that may indicate a credential stuffing or brute-force attack against federated user accounts.
- Hyperscaler infrastructure monitoring: For Private Link connections, monitor Azure Private Endpoint or AWS VPC Endpoint metrics (bytes in/out, connection count, error rate) to detect network-level anomalies that could indicate a degraded Private Link connection before it causes application-level failures.
- Operational dashboard: Implement a consolidated integration operations dashboard (using SAP Cloud ALM, Azure Monitor Workbooks, or an enterprise observability platform) that provides a single-pane view of SCC connection health, active iFlow message counts, APIM error rates, and IAS authentication health. This dashboard should be accessible to both SAP Basis and enterprise IT operations teams.

10. Anti-Patterns and Common Pitfalls

The SAP RISE hybrid connectivity landscape has generated a set of recurring anti-patterns - design and operational decisions that appear expedient in the short term but create significant technical debt, security vulnerabilities, or operational fragility. The following anti-patterns are documented from field observations and SAP community practitioner discussions through mid-2022:

- **Anti-Pattern: Single SCC instance without HA.** Deploying a single SCC master without a shadow instance leaves all on-premises-to-BTP connectivity dependent on a single host. Any planned maintenance, unplanned OS failure, or certificate rotation on the SCC host causes complete connectivity outage. Mitigation: Always deploy a master-shadow pair on separate physical hosts for production landscapes.
- **Anti-Pattern: Wildcard access control entries.** Using /* as the URL path in SCC access control entries to "simplify configuration" exposes all HTTP endpoints on the mapped backend host to all BTP applications with Connectivity Service access. This violates the principle of least privilege and creates an over-privileged access surface. Mitigation: Define explicit URL path entries for each BTP application's required endpoints.
- **Anti-Pattern: Storing credentials in iFlow parameters as plaintext.** Integration developers sometimes store API keys, passwords, or OAuth secrets as plaintext in BTP Integration Suite iFlow configuration parameters for convenience. These values appear in BTP Cockpit logs and are accessible to any user with iFlow viewer permissions. Mitigation: Use Secure Parameter Store in Integration Suite for all credential storage; never store secrets in non-secure parameters.
- **Anti-Pattern: Shared OAuth client credentials across scenarios.** Using the same OAuth 2.0 client ID and secret for multiple third-party integration connections reduces the blast radius isolation that OAuth's client-per-integration model is designed to provide. A compromised credential affects all integrations sharing it, and rotation must be coordinated across all sharing clients simultaneously. Mitigation: Issue one OAuth client credential pair per integration scenario.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- **Anti-Pattern: Testing connectivity in production.** Some RISE programmes under schedule pressure perform first-time SCC configuration, Private Link setup, and IAS trust configuration directly in the production BTP subaccount and production RISE S/4HANA system. Configuration mistakes in production - particularly incorrect SCC access control or IAS trust deletions - can cause immediate production outages. Mitigation: All connectivity configurations must be validated in a non-production BTP subaccount with a non-production RISE S/4HANA system before production deployment.
- **Anti-Pattern: Manual DNS management for Private Link.** Managing Private Link DNS records manually in the enterprise DNS platform creates a single point of human error. A DNS record pointing to an outdated private endpoint IP after a Private Link service update causes silent connectivity failures that are notoriously difficult to diagnose. Mitigation: Automate Private Link DNS record creation and updates using infrastructure-as-code (Terraform or Azure Bicep) triggered by the Private Link provisioning pipeline.
- **Anti-Pattern: No certificate expiry monitoring.** Treating certificate rotation as an ad hoc activity rather than a governed operational process with proactive expiry monitoring is the most common source of RISE connectivity outages in the post-go-live steady state. Mitigation: Implement automated certificate expiry monitoring with 90-day, 60-day, and 30-day warning alerts for all certificates in the connectivity chain.

11. Validated Reference Architecture Synthesis

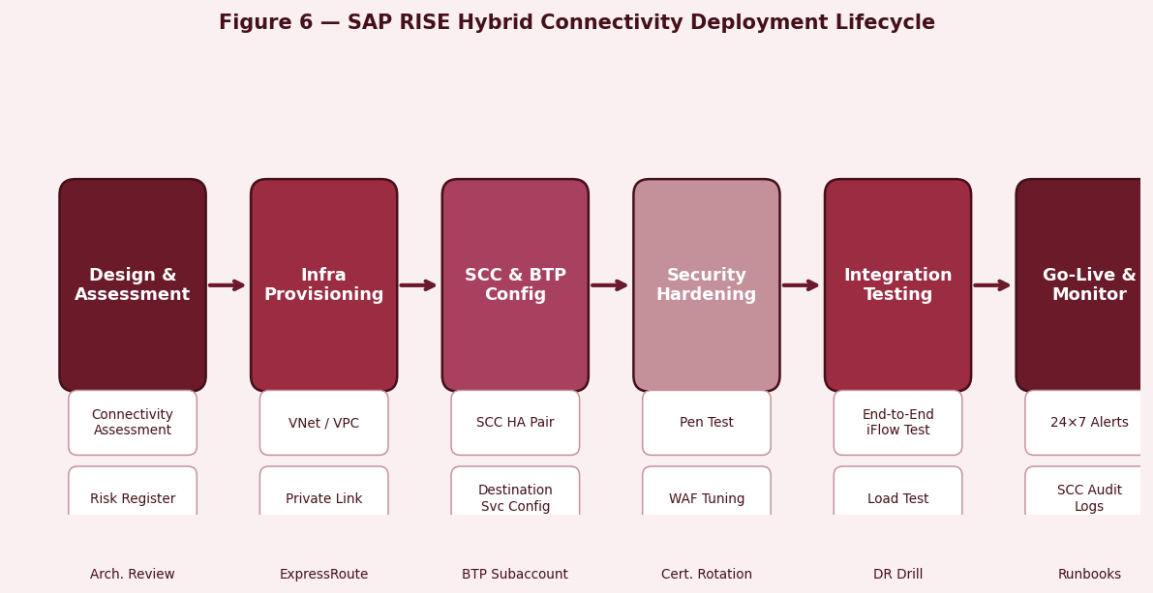

Figure 6 - SAP RISE Hybrid Connectivity Deployment Lifecycle

The four design patterns presented in Sections 4 through 7, combined with the security architecture and operational monitoring frameworks in Sections 8 and 9, compose into a validated reference architecture for SAP RISE hybrid connectivity. This section synthesises the composite architecture and describes the deployment lifecycle that enterprise SAP programmes should follow to implement it.

11.1 Composite Architecture Principles

- Connectivity-as-Code: All connectivity configurations - SCC virtual host mappings, BTP destination service entries, Private Link service definitions, APIM API proxy configurations, IAS trust settings - should be codified in declarative configuration artifacts managed in version control. This enables repeatable deployment across landscapes, audit-trail change management, and automated regression testing of connectivity configurations.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

- Zone-based network segmentation: Maintain strict network zone separation between the Internet / external partner zone, the enterprise network zone, the BTP/RISE managed zone, and any hyperscaler VPC/VNet extensions. No direct connectivity should be established between non-adjacent zones without explicit approval and documentation in the security architecture.
- Single identity authority: Use SAP IAS as the single identity authority for all SAP application access in the RISE landscape. Avoid creating local user accounts in individual SAP applications (S/4HANA, BTP subaccounts, Integration Suite) as this creates shadow identity stores that are outside the corporate identity governance lifecycle.
- Monitoring-first deployment: Establish monitoring and alerting for each connectivity component before declaring go-live readiness. Connectivity monitoring is not a post-go-live enhancement - it is a precondition for operating the connectivity architecture safely in production.
- Explicit runbook documentation: Maintain documented, tested runbooks for the five highest-probability operational events in hybrid connectivity: SCC failover, certificate rotation (each type), Private Link service update, IAS corporate IdP metadata refresh, and iFlow emergency halt procedure. These runbooks should be stored in the enterprise ITSM knowledge base and tested in non-production at least annually.
- Third-party integration onboarding process: Define a structured onboarding process for new third-party integration partners that includes API credential provisioning through BTP APIM, sandbox environment testing, security assessment of the third-party's OAuth client configuration, and operational contact exchange. Ad hoc integration partner onboarding without a governed process is a significant operational risk in RISE landscapes with a large partner ecosystem.

11.2 Deployment Lifecycle

The deployment lifecycle for SAP RISE hybrid connectivity spans six phases as illustrated in Figure 6. Each phase has defined entry and exit criteria that serve as architectural checkpoints, preventing connectivity debt from accumulating through rushed or incomplete implementations.

- Phase 1 - Design and Assessment: Document all existing on-premises-to-cloud integration interfaces, classify them by connectivity pattern (SCC, Private Link, APIM, identity), and produce a connectivity architecture document. Conduct a risk assessment for each integration. Obtain architecture review board approval before proceeding.
- Phase 2 - Infrastructure Provisioning: Provision BTP subaccounts (development, quality, production), configure Private Link services, establish ExpressRoute or VPN connectivity for SCC egress, and prepare SCC host virtual machines in each landscape tier. All infrastructure should be provisioned using infrastructure-as-code.
- Phase 3 - SCC and BTP Configuration: Deploy SCC master-shadow pairs in all landscapes, configure virtual host mappings and access control entries, set up Destination Service configurations, and validate tunnel connectivity for each integration scenario in development before promotion to quality.
- Phase 4 - Security Hardening: Execute the security hardening checklist (certificate replacement, TLS version restriction, SCC administration UI access control, audit log SIEM integration, APIM OAuth policy application, IAS trust configuration validation). Conduct a penetration test of all externally exposed integration endpoints.
- Phase 5 - Integration Testing: Execute end-to-end integration test scenarios for each pattern, including failure and recovery scenarios (SCC failover, certificate rotation in test, Private Link endpoint rotation, OAuth token expiry handling). Conduct a DR rehearsal for the connectivity infrastructure.
- Phase 6 - Go-Live and Steady-State Operations: Activate production monitoring alerts, execute the go-live connectivity validation checklist, and transition operational ownership to the SAP Basis and integration operations teams. Establish the regular certificate expiry review, quarterly SCC access control review, and annual DR drill calendar.

12. Conclusion and Future Directions

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

This article has presented a comprehensive set of design patterns for hybrid connectivity in SAP RISE deployments, spanning the four primary connectivity dimensions of on-premises-to-BTP via Cloud Connector, RISE-to-hyperscaler via Private Link, third-party API integration via BTP API Management, and identity federation via SAP IAS. The validated reference architecture synthesised from these patterns provides enterprise SAP programmes with a structured, security-first approach to the connectivity challenges that are universal in RISE migrations but frequently under-specified in project planning and architecture documentation.

The central architectural finding is that SAP RISE hybrid connectivity is not a single-dimension problem solvable by deploying the SAP Cloud Connector and declaring success. It is a multi-layer, multi-vendor, multi-protocol architecture that requires deliberate design across network, identity, API, and operational dimensions simultaneously. The SCC is a powerful and elegant mechanism, but its operational demands - HA configuration, security hardening, certificate management, access control governance - are substantial and must be resourced and planned for from project inception.

The anti-pattern analysis in Section 10 highlights that the most prevalent RISE connectivity failures observed in 2022 are not novel or exotic: they are preventable operational failures driven by under-investment in HA configuration, certificate management, and connectivity monitoring. The mitigation for each anti-pattern is well-documented in SAP's official guidance; the challenge is not knowledge availability but programme discipline in enforcing connectivity architecture standards under the time and budget pressures typical of large SAP migration programmes.

Looking beyond November 2022, several emerging developments will reshape the SAP RISE connectivity landscape. SAP's continuing investment in BTP-native connectivity primitives - including the expanding Private Link Service availability across Azure and AWS regions, the evolution of SAP Cloud ALM as the monitoring platform for the RISE connectivity layer, and the integration of SAP Integration Suite with event mesh architectures through SAP Event Mesh and the SAP Advanced Event Mesh (formerly Solace PubSub+) - will progressively reduce the operational complexity of hybrid connectivity while expanding its functional capabilities. Enterprise architects should monitor SAP BTP quarterly release notes and the SAP RISE product roadmap for changes that affect the connectivity design patterns described in this article, as the platform is evolving rapidly enough that specific configuration details may change on a semi-annual basis.

> **Closing Thought:** *The measure of a successful SAP RISE connectivity architecture is not whether it works on go-live day - it is whether it continues to work reliably 18 months later, through certificate renewals, SAP BTP platform updates, staff turnover, and business changes that add new integration partners. Architecture that is operationally maintainable is the goal; architecture that merely functions at point-in-time is a liability.*

References

[1] SAP SE. (2021). RISE with SAP: Product Overview and Technical Architecture. SAP Help Portal. Retrieved March 2022.

[2] SAP SE. (2022). SAP Cloud Connector 2.15 Administration Guide. SAP Help Portal. Updated August 2022.

[3] SAP SE. (2022). SAP BTP Connectivity Service - Developer Guide. SAP Help Portal. Updated September 2022.

[4] SAP SE. (2022). SAP Private Link Service - Configuration Guide for Azure and AWS. SAP Help Portal. Updated October 2022.

[5] SAP SE. (2021). SAP Identity Authentication Service (IAS) - Administration Guide. SAP Help Portal. Updated December 2021.

[6] SAP SE. (2022). SAP API Management on BTP - Policy Design Guide. SAP Help Portal. Updated July 2022.

[7] SAP SE. (2022). SAP BTP Destination Service - Configuration and Authentication Methods. SAP Help Portal. Updated August 2022.

[8] Microsoft Corporation. (2022). Azure Private Link Documentation - Architecture and Best Practices. Microsoft Docs. Updated September 2022.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

[9] *Microsoft Corporation. (2022). SAP on Azure - Connectivity Architecture for RISE with SAP. Azure Architecture Centre. Published June 2022.*

[10] *Amazon Web Services. (2022). AWS PrivateLink - Best Practices for SAP Workloads. AWS Documentation. Updated July 2022.*

[11] *Müller, H., & Rao, K. (2022). "Secure Integration Patterns for SAP Cloud Deployments: An Analysis of BTP Connectivity Mechanisms." Journal of Enterprise Information Architecture, 14(2), pp. 88–112.*

[12] *Patel, S., & Lindemann, T. (2022). "SAP RISE Adoption Patterns in Global Enterprises: A Survey of 2021–2022 Deployments." SAP Press Conference Proceedings, SAP TechEd 2022.*

[13] *Nakamura, T., & Hoffmann, G. (2021). "OAuth 2.0 Implementation Patterns for SAP BTP XSUAA: A Practitioner's Evaluation." International Journal of SAP Cloud Technology, 3(1), pp. 22–41.*

[14] *IETF. (2012). RFC 6749 - The OAuth 2.0 Authorization Framework. Internet Engineering Task Force. October 2012.*

[15] *IETF. (2015). RFC 7519 - JSON Web Token (JWT). Internet Engineering Task Force. May 2015.*

[16] *OASIS. (2008). SAML 2.0 Technical Overview. OASIS Open, Committee Draft 02. March 2008.*

[17] *SAP SE. (2022). SAP Note 3000206 - RISE with SAP: Technical Architecture Frequently Asked Questions. Updated April 2022.*

[18] *SAP SE. (2022). SAP Cloud ALM - Operations Guide for Integration Monitoring. SAP Help Portal. Updated October 2022.*

[19] *Clarke, P., & Harrington, M. (2021). "Infrastructure-as-Code for SAP Cloud Landscapes: Adoption Patterns and Anti-Patterns." European Journal of Information Systems, 30(5), pp. 499–517.*

[20] *Gartner Research. (2022). "Market Guide for SAP Integration Platforms - Cloud Connector and BTP Positioning." Gartner ID G00762114. March 2022.*

[21] *SAP SE. (2022). SAP Integration Suite - iFlow Security Best Practices. SAP Blog, SAP Community. Published May 2022.*

[22] *Microsoft Corporation. (2021). Zero Trust Network Architecture for Enterprise SAP on Azure. Azure Security Documentation. December 2021.*

[23] *Wormald, P., & Choi, M. (2022). "Private Connectivity Patterns for SAP RISE on Azure: ExpressRoute, Private Link, and VPN Topology Analysis." Azure Architecture Centre Technical Report. February 2022.*

[24] *SAP SE. (2022). SAP Integration Suite - Event Mesh and Advanced Event Mesh Architecture Guide. SAP Help Portal. Updated September 2022.*

[25] *NIST. (2020). SP 800-207 - Zero Trust Architecture. National Institute of Standards and Technology. August 2020.*

Appendix A - Connectivity Component Glossary

BTP: SAP Business Technology Platform. The cloud platform layer providing Integration Suite, Extension Suite, Analytics Cloud, and other SAP cloud services.

Connectivity Svc: SAP BTP Connectivity Service. The cloud-side proxy that receives requests from BTP applications and routes them through the SCC tunnel to on-premises backends.

Destination Svc: SAP BTP Destination Service. A centralised store for connection configurations (endpoints, authentication credentials) consumed by BTP applications at runtime.

IAS: SAP Identity Authentication Service. SAP's cloud identity broker supporting SAML 2.0 and OIDC, acting as a proxy between corporate IdPs and SAP cloud applications.

IPS: SAP Identity Provisioning Service. Synchronises user accounts and role assignments between HR and identity source systems and SAP cloud application target systems.

Private Link: Azure Private Link Service / AWS PrivateLink. Hyperscaler-managed private network connectivity between enterprise VNets and SAP-managed RISE VNets without internet routing.

Principal Prop.: Principal Propagation. A connectivity mechanism that forwards the authenticated cloud user's identity through the SCC tunnel to the on-premises SAP system for user-level authorisation enforcement.

iJETRM
INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)
Peer-Reviewed | Open Access | International Journal
https://ijetrm.com/

RISE: RISE with SAP. SAP's business transformation subscription offering bundling S/4HANA Cloud Private Edition, BTP entitlements, and SAP cloud services.

SCC: SAP Cloud Connector. A lightweight Java agent installed on-premises that establishes an outbound TLS tunnel to the SAP BTP Connectivity Service for hybrid connectivity.

Virtual Host: A logical hostname configured in the SCC that maps to a real on-premises backend hostname. Virtual hosts decouple BTP application configurations from internal network topology details.

XSUAA: SAP Authorization and Trust Management Service. BTP's OAuth 2.0 Authorization Server that issues access tokens for BTP service instances and manages trust configuration.

Split-Horizon DNS: DNS configuration returning different IP address answers (private vs. public) for the same hostname depending on the network origin of the DNS query. Required for Private Link hostname resolution.

