Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Unified Identity Management in the Cloud: SAP IAS Integration with SAP BTP

Srinivas Kolluri
Quantum Integrators Group LLC, USA
Corresponding Author: Srinivas Kolluri, **E-mail**: skolluri842@gmail.com

| ABSTRACT

SAP Identity Authentication Service (IAS) integration with SAP Business Technology Platform (BTP) provides enterprise-grade identity management for distributed cloud environments. Built on SAP NetWeaver AS ABAP infrastructure, the solution delivers secure authentication, authorization, and identity governance through standardized protocols and security controls. The integration framework enables unified access management across cloud and on-premise applications through sophisticated token management, policy enforcement, and audit mechanisms. The implementation supports diverse authentication methods, including SAML federation, X.509 certificates, and OAuth protocols, while maintaining security compliance and operational efficiency. The framework implements comprehensive security control, including encrypted communication channels, certificate-based trust relationships, and granular access management policies. Through standardized integration patterns and automated monitoring capabilities, organizations can maintain consistent security controls while supporting various deployment scenarios, including hybrid cloud and multi-tenant environments.

| KEYWORDS

Identity federation, Authentication protocols, Enterprise security, Cloud integration, Access governance

| ARTICLE INFORMATION

ACCEPTED: 19 May 2025 **PUBLISHED:** 03 June 2025 **DOI:** 10.32996/jcsts.2025.7.5.73

1. Introduction

In the era of digital transformation, enterprises require robust identity management solutions that can effectively secure their distributed cloud environments. The integration between SAP Identity Authentication Service (IAS) and SAP Business Technology Platform (BTP) delivers this capability through a comprehensive security architecture built on SAP NetWeaver AS ABAP infrastructure. This foundation provides enterprise-grade security features specifically designed for SAP landscapes, implementing sophisticated authentication mechanisms that protect both cloud and on-premise resources [1].

The SAP NetWeaver AS ABAP security infrastructure forms the core of the authentication framework, implementing SAP's Single Sign-On 3.0 protocol for secure system access. This infrastructure utilizes the Secure Network Communications (SNC) layer for encrypted data transmission, ensuring that all authentication traffic between systems remains protected. The SNC implementation supports various security products and maintains compatibility with industry-standard security protocols, enabling seamless integration with existing enterprise security infrastructure [2].

Integration with S/4HANA Cloud extends the security framework to modern cloud deployments through standardized interfaces and protocols. The system implements multiple authentication mechanisms to support diverse enterprise requirements. These include traditional username and password authentication enhanced with modern security features, X.509 client certificates for strong authentication, SAML 2.0 federation for seamless single sign-on across applications, and Kerberos authentication for integrated Windows authentication scenarios [15].

The security architecture implements concrete protocols and standards that ensure consistent protection across the enterprise landscape. The SAML 2.0 implementation supports secure identity federation with certificate-based trust relationships and encrypted assertions. X.509 certificate authentication utilizes strong cryptographic algorithms with a minimum 2048-bit key length and secure hash functions. The Kerberos integration supports AES encryption for ticket protection, ensuring robust security for Windows-integrated authentication scenarios [2].

System requirements for implementing this security framework include specific infrastructure components that ensure proper authentication handling. The SAP Cryptographic Library must be installed and properly configured on all systems participating in the authentication process. Network infrastructure must support secure communication protocols, including TLS 1.2 or higher for all system connections. Firewall configurations must allow communication on specific ports for authentication traffic while maintaining proper security boundaries [15].

Network security requirements extend beyond basic connectivity to ensure comprehensive protection of authentication processes. This includes implementing reverse proxy servers for external access, maintaining proper network segmentation between security zones, and ensuring encrypted communication channels for all authentication traffic. The infrastructure must support proper certificate management, including automated rotation and renewal processes to maintain continuous security protection [1].

The framework's implementation in modern cloud environments, particularly with S/4HANA Cloud, introduces additional security considerations for protecting cloud-based resources. This includes supporting OAuth 2.0 protocols for API authentication, implementing proper principal propagation for maintaining user context across system boundaries, and ensuring secure service-to-service communication through certificate-based authentication. These capabilities enable organizations to maintain consistent security controls across their hybrid landscape while supporting modern application architectures [15].

2. Technical Architecture Framework

The technical architecture of SAP Identity Authentication Service (IAS) integration with SAP Business Technology Platform (BTP) encompasses several sophisticated components that work together to provide comprehensive identity management capabilities. This framework builds upon SAP's proven security infrastructure while incorporating modern authentication mechanisms suitable for cloud and hybrid deployments [3].

2.1 SAP SSO 3.0 Components

The Secure Network Communication (SNC) layer serves as a fundamental component of the authentication framework. The system requires specific configuration within the /usr/sap/DVEBMGS00/sec directory, where core security components are maintained. The SNC implementation relies on the SAP Cryptographic Library, which must be properly configured through the SNC_LIB parameter pointing to the sapcrypto. so library. Security quality of protection is enforced through the SNC_QOP parameter set to level 3, ensuring maximum security for all communications. The SECUDIR environment variable must reference the security directory to enable proper cryptographic operations [3].

Digital certificate management forms another crucial aspect of the security infrastructure. The Personal Security Environment (PSE) files are maintained within the designated security directory at /usr/sap/DVEBMGS00/sec. These certificates must meet stringent security requirements, including a minimum key length of 2048 bits to ensure adequate cryptographic strength. The system enforces the use of SHA256 for digital signatures, providing strong cryptographic protection for all signed content. Certificates are managed with a standard validity period of two years, requiring proper renewal processes to maintain continuous security coverage [3].

2.2 Authentication Flow

The authentication process implements a sophisticated token-based approach utilizing SAP Logon and Assertion Tickets. These tokens follow a standardized format that ensures interoperability across the SAP landscape while maintaining strong security controls. The system supports configurable token validity periods, with a default setting of eight hours that balances security requirements with user convenience. All token-related cryptographic operations utilize AES-256 encryption, ensuring strong protection of authentication credentials and session information [4].

2.3 System Trust Configuration

Trust relationships between systems are managed through a comprehensive trust configuration framework. The trust store, located at /usr/sap/SID/profile, maintains all necessary certificates and trust anchors for secure system communication. The configuration requires specific parameters for both client and server communications, implemented through carefully defined cipher suite selections. These parameters ensure that all system communications utilize appropriate encryption algorithms and security protocols [4].

The ssl/client_ciphersuites parameter defines allowed encryption algorithms for client connections, while ssl/server_ciphersuites specifies acceptable algorithms for server operations. The general ssl/ciphersuites parameter provides default settings that apply when specific client or server parameters are not defined. This layered approach to cipher suite configuration enables organizations to implement appropriate security controls while maintaining compatibility with various system components [4].

The technical architecture implements additional security controls through the Profile Security Entity framework. This component manages security configurations across the system landscape, ensuring consistent application of security policies and authentication requirements. The framework supports dynamic updates to security configurations while maintaining system stability and ensuring continuous availability of authentication services [3].

Certificate lifecycle management is integrated into the framework through automated processes that monitor certificate validity and trigger renewal procedures when needed. This includes management of root certificates, intermediate certificates, and end-entity certificates used for various authentication scenarios. The system maintains proper certificate chains and validates all certificates against current revocation information to ensure continued security of authentication processes [4].

Element	Configuration	Security Parameters
SNC Layer	Security Directory	Cryptographic Settings
PSE Files	Certificate Storage	Key Requirements
Trust Store	System Profiles	Cipher Configurations
Authentication Flow	Token Management	Encryption Standards

Table 1: SAP SSO Implementation Components [3,4]

3. Integration Solution Components

The integration solution components for SAP Identity Authentication Service establish sophisticated patterns for connecting with S/4HANA Cloud and managing secure communication across the enterprise landscape. These components implement standardized integration protocols while maintaining robust security controls throughout the communication chain [5].

3.1 S/4HANA Cloud Integration

Integration with S/4HANA Cloud requires precise configuration of communication scenarios that enable secure system interaction. The framework implements the SAP_COM_0008 communication scenario, which provides standardized interfaces for business partner integration. This scenario definition includes comprehensive security controls and communication parameters that ensure proper system integration while maintaining data security [5].

Technical user configuration within the integration framework requires specific role assignments that control system access capabilities. The SAP_BR_BUPA_MASTER_SPECIALIST role provides necessary authorizations for business partner data management, implementing proper segregation of duties through granular permission controls. The S_SERVICE authorization object manages service-level access, controlling system capabilities through defined authorization parameters [5].

OAuth configuration within the integration framework implements modern security protocols for service authentication. The system utilizes a dedicated OAuth token endpoint at /oauth2/token for managing authentication credentials. Access scopes, particularly the API_BUSINESS_PARTNER scope, control specific API access rights, ensuring that system communications remain properly constrained to authorized operations. This OAuth implementation supports secure service-to-service communication while maintaining proper audit trails of all authentication activities [5].

3.2 Principal Propagation

Principal propagation enables seamless transmission of user identity information across integrated systems while maintaining the security context. The configuration implements specific parameters that control communication behavior and security settings. The framework utilizes Internet proxy types for external communication, ensuring proper routing of authentication traffic through secured channels [6].

Authentication mechanisms within the principal propagation framework specifically utilize the PrincipalPropagation method, enabling secure transmission of identity information between systems. This implementation requires proper OAuth client registration, establishing secure service identities that support automated system communication. The framework maintains

detailed records of client registrations and authentication activities, supporting proper security monitoring and audit requirements [6].

Trust configuration for principal propagation relies on sophisticated certificate management processes. The framework implements X.509 certificate exchange procedures that establish secure trust relationships between communicating systems. These certificates must meet specific security requirements, including appropriate key lengths, proper certificate attributes, and validated trust chains. The system maintains automated certificate management processes that ensure the timely renewal of certificates while maintaining secure communication channels [6].

SAML trust configuration provides an additional layer of security for identity federation scenarios. The framework supports detailed configuration of SAML trust relationships, including proper specification of identity providers, service providers, and required security attributes. This SAML implementation enables secure single sign-on capabilities while maintaining proper security controls throughout the authentication process [6].

The integration framework includes comprehensive monitoring capabilities that track system communication status and security parameters. These monitoring functions maintain detailed logs of integration activities, enabling effective troubleshooting and security analysis when required. The framework supports automated alerts for communication issues, certificate expiration, and other security-relevant events, ensuring proper maintenance of integration security [5].

Component	Implementation	Security Controls
Communication Scenarios	Business Partner APIs	Authorization Objects
Principal Propagation	Identity Transmission	Trust Configuration
OAuth Implementation	Token Management	Access Scopes
Monitoring	System Status	Security Alerts

Table 3: S/4HANA Cloud Integration Architecture [5,6]

4. Implementation Framework

The implementation framework for SAP Identity Authentication Service defines concrete patterns for establishing secure authentication and system communication. This framework encompasses both SAML-based federation and system-level communication configurations, ensuring secure and reliable integration across the enterprise landscape [7].

4.1 SAML Configuration

SAML implementation within SAP IAS requires precise configuration of identity provider services through standardized endpoints and protocols. Each tenant maintains a dedicated metadata endpoint accessible through a structured URL format at https://<tenant>.accounts.ondemand.com/saml2/metadata. This endpoint serves as the authoritative source for federation configuration information, providing essential details for service provider integration and trust establishment [7].

The SAML framework supports multiple protocol bindings to accommodate various integration scenarios. HTTP-POST binding enables secure transmission of larger SAML messages, particularly important for handling signed assertions and complex authentication data. HTTP-Redirect binding provides an alternative mechanism suitable for simpler authentication flows, while maintaining security through proper message protection. These binding options ensure flexibility in integration while maintaining consistent security controls [7].

Security requirements within the SAML implementation mandate encryption of assertions to protect sensitive authentication information. The framework enforces RSA-SHA256 as the signature algorithm for all SAML messages, ensuring strong cryptographic protection of authentication data. This combination of assertion encryption and digital signatures provides comprehensive protection for authentication information throughout the federation process [7].

4.2 System Communication

System communication configuration implements structured approaches for establishing secure connections between integrated systems. The destination configuration utilizes HTTP as the transport protocol, with endpoints following the standardized pattern https://<tenant>.s4hana.ondemand.com for S/4HANA Cloud integration. This configuration ensures proper routing of system communications while maintaining security through encrypted channels [8].

OAuth 2.0 serves as the primary authentication mechanism for system communication, implementing modern security protocols for service authentication. This approach enables secure service-to-service communication while supporting automated processes and system integration scenarios. The OAuth implementation includes comprehensive token management and validation processes, ensuring secure handling of authentication credentials throughout the communication lifecycle [8].

Communication arrangements within the system follow standardized patterns defined through specific scenario identifiers. The SAP_COM_0008 scenario provides a standardized framework for business partner integration, implementing well-defined security parameters and communication protocols. This scenario utilizes the API_BUSINESS_PARTNER service interface, enabling secure access to business partner data while maintaining proper access controls [8].

The implementation framework includes sophisticated monitoring capabilities that track communication status and security parameters. These monitoring functions maintain detailed logs of system interactions, enabling effective troubleshooting and security analysis. The framework supports automated alerting for communication issues, security events, and performance metrics, ensuring proper maintenance of system integration [7].

Security controls within the implementation framework extend beyond basic authentication to include comprehensive protection of communication channels. This includes certificate validation, token lifecycle management, and continuous monitoring of security parameters. The framework maintains detailed audit trails of all communication activities, supporting security compliance requirements and enabling effective incident response [8].

Configuration	Protocol Features	Security Measures
Identity Provider	Metadata Endpoints	Assertion Encryption
Protocol Bindings	Message Handling	Digital Signatures
System Communication	Transport Security	OAuth Integration
Monitoring	Security Events	Audit Trails

Table 4: Authentication Protocol Implementation [7,8]

5. Security Framework

The security framework within SAP Identity Authentication Service implements comprehensive controls that protect authentication processes and identity data. This framework establishes concrete security parameters, certificate management procedures, and audit mechanisms that work together to maintain system security while supporting operational requirements [9].

5.1 Security Configuration

Password security represents a foundational element of the authentication framework, implementing stringent policies that align with enterprise security requirements. The system enforces a minimum password length of twelve characters, providing adequate complexity to resist unauthorized access attempts. Password composition rules mandate the inclusion of uppercase and lowercase letters, numbers, and special characters, ensuring the creation of strong passwords that meet modern security standards [9].

Password history controls maintain security through the prevention of password reuse, storing the previous twenty-four passwords for each user account. This mechanism ensures that users create unique passwords when changes are required, enhancing overall security through password diversity. The framework implements a maximum password age of ninety days, requiring regular password updates while balancing security requirements with user experience considerations [9].

The security configuration extends beyond password policies to encompass comprehensive access controls and security parameters. These controls implement proper segregation of duties, ensuring that administrative functions remain properly restricted to authorized personnel. The framework maintains detailed security policies that govern system access, authentication requirements, and security monitoring functions [9].

5.2 Certificate Management

Certificate management within the security framework utilizes SAP's Personal Security Environment (PSE) system for maintaining digital certificates and cryptographic keys. The sapgenpse utility provides essential functionality for managing these security components, with the maintain_pk command enabling secure creation and maintenance of PSE files. This command requires

specific parameters, including the PSE file location, PIN protection for private keys, and proper specification of certificate request files [10].

The certificate management process implements secure handling of cryptographic materials throughout their lifecycle. Private keys remain protected through PIN-based encryption, ensuring secure storage of sensitive cryptographic components. The framework supports automated certificate management processes, including renewal notifications, certificate deployment, and proper revocation handling when required [10].

Trust establishment through certificate management follows standardized procedures that ensure proper security controls. The framework supports various certificate type,s including server certificates, client certificates, and certificate authority certificates. These certificates must meet specific security requirements including appropriate key lengths, validated trust chains, and proper specification of certificate attributes [9].

5.3 Audit Configuration

The audit framework maintains comprehensive logging of security-relevant events through a structured logging system. Audit logs are maintained in the designated system path at /usr/sap/SID/log, providing centralized storage of security audit information. The framework implements specific audit parameters that control logging behavior and ensure capture of relevant security events [10].

Security audit logging activation occurs through the rsau/enable parameter, ensuring proper recording of security events. The framework supports user-specific audit logging through the rsau/user_selection parameter, enabling focused monitoring of specific user activities when required for security investigations. The system maintains multiple selection slots through the rsau/selection_slots parameter, supporting sophisticated filtering of audit events based on various criteria [10].

Audit log management includes comprehensive controls for protecting audit information and maintaining proper log retention. The framework implements encryption for sensitive audit data and maintains proper access controls for audit logs. These measures ensure the integrity and confidentiality of audit information while supporting security monitoring and compliance requirements [9].

The security framework includes sophisticated monitoring capabilities that track security events and system status. These monitoring functions maintain detailed logs of security activities, enabling effective incident response and security analysis. The framework supports automated alerting for security events, compliance violations, and system status changes, ensuring proper maintenance of security controls [10].

6. Integration Patterns

The integration patterns within SAP Identity Authentication Service establish standardized approaches for connecting enterprise systems and managing secure data exchange. These patterns focus particularly on S/4HANA integration and process management capabilities, implementing secure and efficient communication channels across the enterprise landscape [11].

6.1 S/4HANA Integration Patterns

Business partner integration represents a fundamental integration pattern within the S/4HANA landscape, implementing standardized interfaces for managing business partner data. The API_BUSINESS_PARTNER interface provides comprehensive capabilities for accessing and managing business partner information while maintaining proper security controls. This interface implements standardized REST-based communication patterns, ensuring consistent data access across integrated systems [15].

The integration framework supports specific API methods for business partner management. The GET /A_BusinessPartner method enables secure retrieval of business partner information, implementing proper authorization controls and data filtering. The POST /A_BusinessPartner method provides capabilities for creating new business partner records, ensuring proper data validation and security checks during record creation [11].

Access control within the business partner integration pattern utilizes OAuth scopes for managing authorization. The API_BUSINESS_PARTNER.read scope provides specific authorization for accessing business partner data, ensuring that system communications remain properly constrained to authorized operations. This OAuth implementation supports secure service-to-service communication while maintaining detailed audit trails of all data access activities [15].

6.2 Process Integration

Process integration through Signavio implements sophisticated patterns for managing business process workflows while maintaining security. The authentication framework utilizes SAML-based federation for securing process access, ensuring proper user authentication and authorization throughout the process lifecycle. This SAML implementation supports single sign-on capabilities while maintaining proper security controls for process management functions [12].

Role-based access control within the process integration framework implements specific roles for managing process activities. The Process Manager role provides comprehensive capabilities for managing process definitions and workflows, including creation, modification, and deletion of process elements. The Process Viewer role enables restricted access for process observation and analysis, implementing proper segregation of duties through granular permission controls [12].

Access control lists within the process integration framework provide detailed control over process resources. These ACLs implement specific permissions for various process components, ensuring proper access control at both the process and element levels. The framework maintains proper separation between different process domains, ensuring that process resources remain properly isolated according to business requirements [11].

The integration patterns include comprehensive monitoring capabilities that track system interactions and process execution. These monitoring functions maintain detailed logs of integration activities, enabling effective troubleshooting and performance analysis. The framework supports automated alerting for integration issues, process exceptions, and performance metrics, ensuring proper maintenance of integration operations [12].

Security controls within the integration patterns extend beyond basic authentication to include comprehensive protection of process data and communication channels. This includes implementation of encrypted communication channels, proper certificate management, and continuous monitoring of security parameters. The framework maintains detailed audit trails of all integration activities, supporting compliance requirements and enabling effective security monitoring [15].

The integration framework supports various deployment scenarios including hybrid cloud implementations and multi-tenant environments. These deployment patterns implement proper resource isolation and security controls while maintaining efficient system integration. The framework provides flexibility in integration approaches while ensuring consistent application of security controls across different deployment scenarios [11].

Pattern	Integration Features	Security Controls
Business Partner	API Methods	OAuth Scopes
Process Management	Role Configuration	Access Control
Deployment Models	Resource Isolation	Security Monitoring
System Integration	Communication Channels	Audit Trails

Table 6: Business Process Integration Architecture [11,12,15]

7. Best Practices and Recommendations

The implementation of SAP Identity Authentication Service (IAS) requires systematic consideration of configuration and integration requirements to ensure successful deployment. When integrating with SAP SuccessFactors and other enterprise applications, organizations must follow specific configuration steps and best practices to establish secure authentication flows. The implementation process includes configuring trust between systems, setting up user authentication, and establishing proper communication channels [13].

Security Considerations

Security configuration for SAP IAS implementations begins with proper trust establishment between systems. Organizations must configure the trust settings in both the Identity Authentication admin console and the integrated applications. This includes uploading the required certificates, configuring the SAML 2.0 endpoints, and establishing the necessary trust relationships. The configuration process requires careful attention to security parameters and proper validation of trust settings [13].

User authentication configuration represents a critical security aspect. SAP IAS supports various authentication methods that must be properly configured according to organizational requirements. The service enables configuration of authentication policies, password policies, and risk-based authentication settings. Organizations should implement appropriate authentication methods based on their security requirements while ensuring proper user access [13].

System communication security requires proper configuration of endpoints and protocols. When integrating with applications like SAP SuccessFactors, organizations must configure the correct service provider endpoints and ensure proper protocol settings. This includes validating the authentication endpoints, configuring single sign-on settings, and establishing secure communication channels between systems [13].

Performance Optimization

Performance optimization in identity and access management systems focuses on ensuring efficient authentication processes. According to IAM principles, identity management systems must handle four key aspects: identification, authentication, authorization, and accountability. These systems play a crucial role in managing user identities and access rights across enterprise resources, requiring proper configuration for optimal performance [14].

Access management configuration requires careful attention to user roles and permissions. IAM systems must implement proper role-based access control (RBAC) mechanisms that define what resources users can access. This includes configuring appropriate user roles, managing access permissions, and implementing proper access control policies across the organization [14].

Resource access patterns must be properly configured to ensure efficient operations. Identity management systems should implement appropriate caching mechanisms and connection management strategies. This includes configuring proper session management settings and implementing efficient authentication flows that maintain both security and performance [14].

Maintenance and Operations

Operational management of identity systems requires comprehensive monitoring and maintenance procedures. Identity management systems must maintain proper audit trails of all authentication and authorization activities. Organizations should implement appropriate logging mechanisms and establish monitoring procedures that provide visibility into system operations [14].

System maintenance procedures should include regular reviews of configuration settings and security policies. IAM systems require ongoing maintenance to ensure they remain aligned with organizational requirements and security policies. This includes regular review of access policies, user roles, and authentication settings to maintain proper security controls [14].

Update management represents an essential operational aspect. Identity management systems must be kept current with security updates and patch management procedures. Organizations should establish clear processes for managing system updates while maintaining proper documentation of all configuration changes and system modifications [14].

Conclusion

The integration between SAP IAS and BTP establishes a robust foundation for managing enterprise identities across hybrid cloud environments. Through standardized security protocols, comprehensive policy enforcement, and sophisticated monitoring capabilities, organizations can implement consistent identity management practices that protect enterprise resources. The solution's support for diverse authentication methods and integration patterns enables secure access to both cloud and on-premise applications while maintaining compliance requirements and operational efficiency. The framework's sophisticated token management and certificate handling ensure secure authentication across distributed systems, while comprehensive audit mechanisms maintain visibility into security events and system operations. Through automated monitoring and alert functions, organizations can promptly identify and respond to security incidents while maintaining system availability. The integration framework's support for various deployment scenarios enables flexible implementation while maintaining consistent security controls. Principal propagation capabilities ensure secure transmission of identity context across system boundaries, while granular access controls enable proper resource protection. The solution's comprehensive approach to identity management, combined with its robust security controls and monitoring capabilities, provides organizations with a secure and scalable foundation for managing enterprise identities in modern cloud environments.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

[1] Carsten Olt, "SAP Identity Authentication Service (IAS) | Overview and Integration Capabilities," Xiting, 2020. [Online]. Available: https://xiting.com/en/sap-identity-authentication-service-overview/

[2] Gartner Peer Insights, " Identity Governance and Administration Reviews and Ratings" 2024. [Online]. Available: https://www.gartner.com/reviews/market/identity-governance-administration

[3] GeeksforGeeks, "Identity and Access Management," 2024. [Online]. Available: https://www.geeksforgeeks.org/identity-and-access-management/
SAP, "SAP S/4HANA Cloud Public Edition", 2024. https://help.sap.com/docs/SAP_S4HANA_CLOUD/9d794cbd48c648bc8a176e422772de7e/7af7b8541486ed05e10000000a4450e5.html

[4] Haddayr Copley-Woods, "Essentials of enterprise identity management," Jamf, 2024. [Online]. Available: https://www.jamf.com/blog/enterprise-identity-management-from-scratch/

[5] IBsolution, "SAP Identity Authentication Service (SAP IAS)," [Online]. Available: https://www.ibsolution.com/en/cyber-security/sap-cloud-identity/sap-identity-authentication-service-sap-ias

[6] Matthew Kosinski, Amber Forrest, "What is identity and access management (IAM)?", IBM, 2024. [Online]. Available: https://www.ibm.com/think/topics/identity-access-management

[7] Phil Sweeney, "What is identity and Access Management (IAM) System? Guide to IAM," TechTarget, 2024. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system

[8] SAP Community, "SAP Cloud Identity Services - Identity Authentication," SAP Community, 2024. [Online]. Available: https://pages.community.sap.com/topics/cloud-identity-services/identity-authentication

[9] SAP Help Portal, "SAP Cloud Identity Services," 2024. [Online]. Available: https://help.sap.com/doc/a7f50a08218845019a5eb5d0ba826691/Cloud/en-US/Identity_Authentication_en.pdf

[10] SAP, "SAP Integrated Report 2023," 2024. [Online]. Available: https://assets.ctfassets.net/z2fsfx60w22m/1BZJuso0mjt0V7vHfB5Niv/cb09d507b131a4057e688e67a01f21d9/SAP_Integrated_Report_2023.pdf

[11] SAP, "System Integration Guide for SAP Cloud Identity Services," SAP Help Portal, 2024. [Online]. Available: https://help.sap.com/docs/cloud-identity/system-integration-guide/identity-authentication-configuration-for-sap-successfactor

[12] Schuyler Brown, "Enterprise Identity & Access Management (IAM) Solutions," StrongDM, 2024. [Online]. Available: https://www.strongdm.com/blog/enterprise-identity-access-management-iam

[13] Surabhi Purwaar, "Demystifying SAP Identity Authentication Service (IAS)," LinkedIn, 2024. [Online]. Available: https://www.linkedin.com/pulse/demystifying-sap-identity-authentication-service-ias-surabhi-purwaar-aou2c/

[14] Zimmergren et al., "Enterprise-scale identity and access management for Azure VMware Solution," Microsoft, 2022. [Online]. Available: https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/azure-vmware/eslz-identity-and-access-management