Application Architecture Icertis

Status	Approved
Owner	CABELLO MARTOS-ext, Gabino
Stakeholders	RUFFINONI, Francois NARCISO, ines DALAL, Shivang
LeanIX Link	Icertis Contract Intelligence

Introduction

Scope & Objectives

The purpose of this document is to describe the architecture of Icertis Contract Intelligence application and the systems it will be integrating with.

Out of Scope:

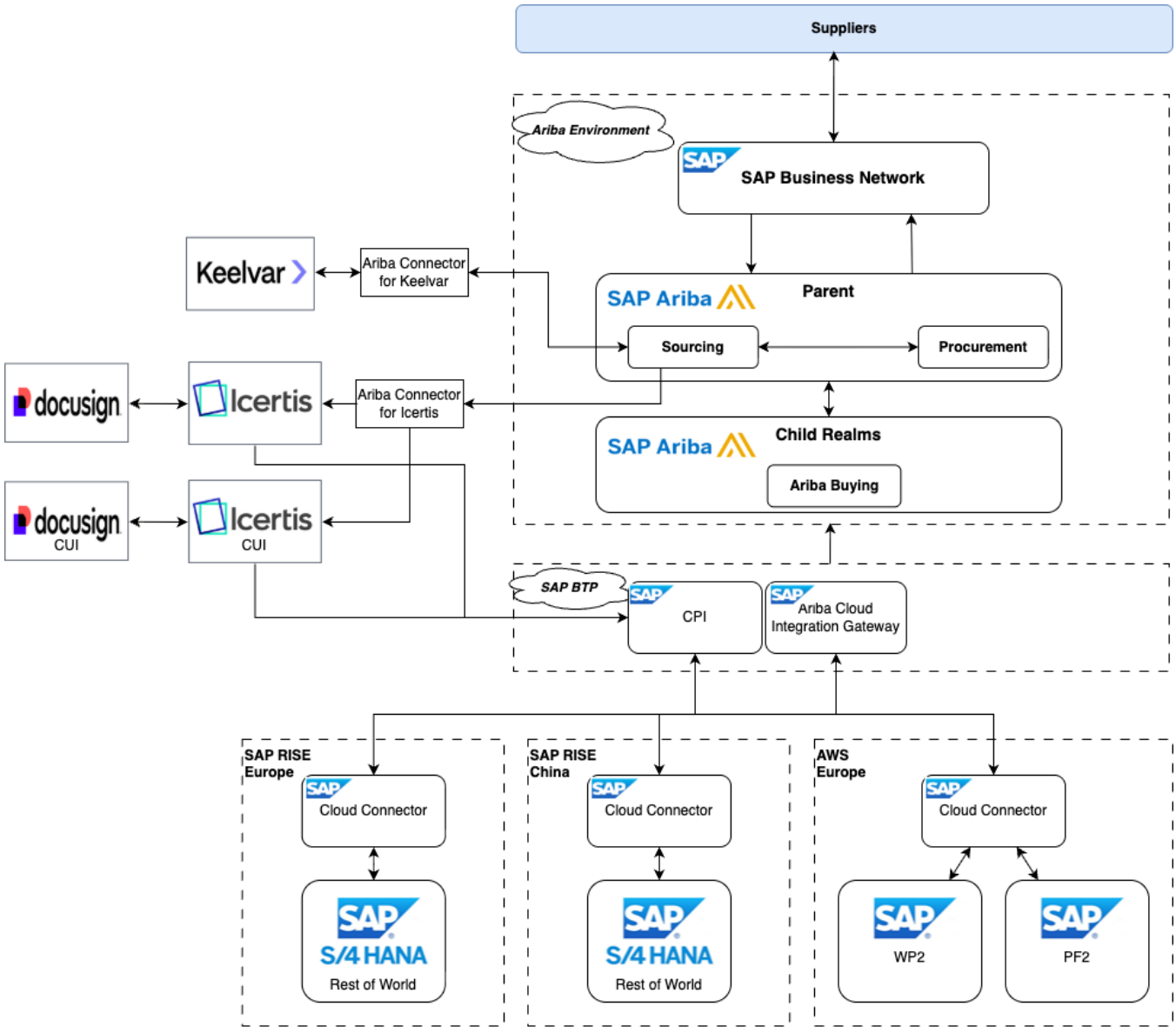
- Since Icertis is a SaaS application, network and infrastructure architecture will be considered as out of Scope.
- Information related to product documentation can be found online will not be documented here, but referenced using hyperlinks.

Key Decisions and Requirements

Description	Rationale
Single Sign-On (SSO)	As part of SyWay project, a common authentication mechanism (e.g., SAML) is adopted for ease of access and unified user experience.
Users must access Icertis using HTTPS.	As part of SyWay standards, all data in transit must be encrypted.
Data stored in Icertis must be encrypted.	As part of SyWay standards, all data at rest to be encrypted.
Icertis must have appropriate data protection.	Icertis performs data backups regularly so that point in time recovery can perform to recover data. Additional, backups must be replicated to another site to protect against a site disaster.
Landscape	Icertis will consist of a three tier landscape of Dev, QA, and Prod.

Application Architecture

Overview



Application Architecture Components

Icertis Contract Intelligence

Icertis is a contract lifecycle management (CLM) platform that helps organizations manage contracts digitally from creation to execution and compliance. It's widely used by enterprises to improve visibility, reduce risk, and ensure compliance across all types of contracts.The "Ariba connector for Icertis" refers to the Icertis Contract Intelligence (ICI) for SAP Ariba integration, which extends SAP Ariba's procurement capabilities with Icertis's advanced contract lifecycle management (CLM) features. This integration synchronizes data between the two platforms, allowing users to manage contracts from sourcing through to payment, leveraging AI and automation for tasks like contract authoring, risk assessment, and compliance tracking.

Ariba Connector for Icertis

The SAP Ariba Connector for Icertis is a packaged, APIbased integration that unifies SAP Ariba sourcing & contracting workflows with Icertis Contract Intelligence (ICI). It enables presignature authoring and negotiation in Icertis, and postsignature contract usage, compliance and visibility in SAP Ariba—so contract data and documents flow reliably across the sourcetopay lifecycle.

System Landscape

ICertis will consist of a three tier landscape. Application will be introduced in with Release 2 of SyWay and later integrated with S/4HANA as part of Release 4. Its use in Release 3 is to be confirmed via a KDD.

Application	Region	SBX	DEV	INT	UAT	PAR	TRG	PROD
ICertis	EU	-	**DEV**			Test	**UAT**	**PRD**
	US*	-	-	Test*				PRD*

*) Subject of a KDD to confirm if required for Release 3.

Application Security

User Access

Icertis is a SaaS application and can be accessed by users over the internet via HTTPS using their web browser. No Syensqo infrastructure or application is required to access Icertis.

User must have their IDs created and assigned with the correct role before they can login to Icertis. Icertis will be integrated in the SAP identity governance and provisioning procedure defined for Syensqo, complete information can be found in Application Architecture Identity Tooling document.

Following are the URLs for Icertis instances:

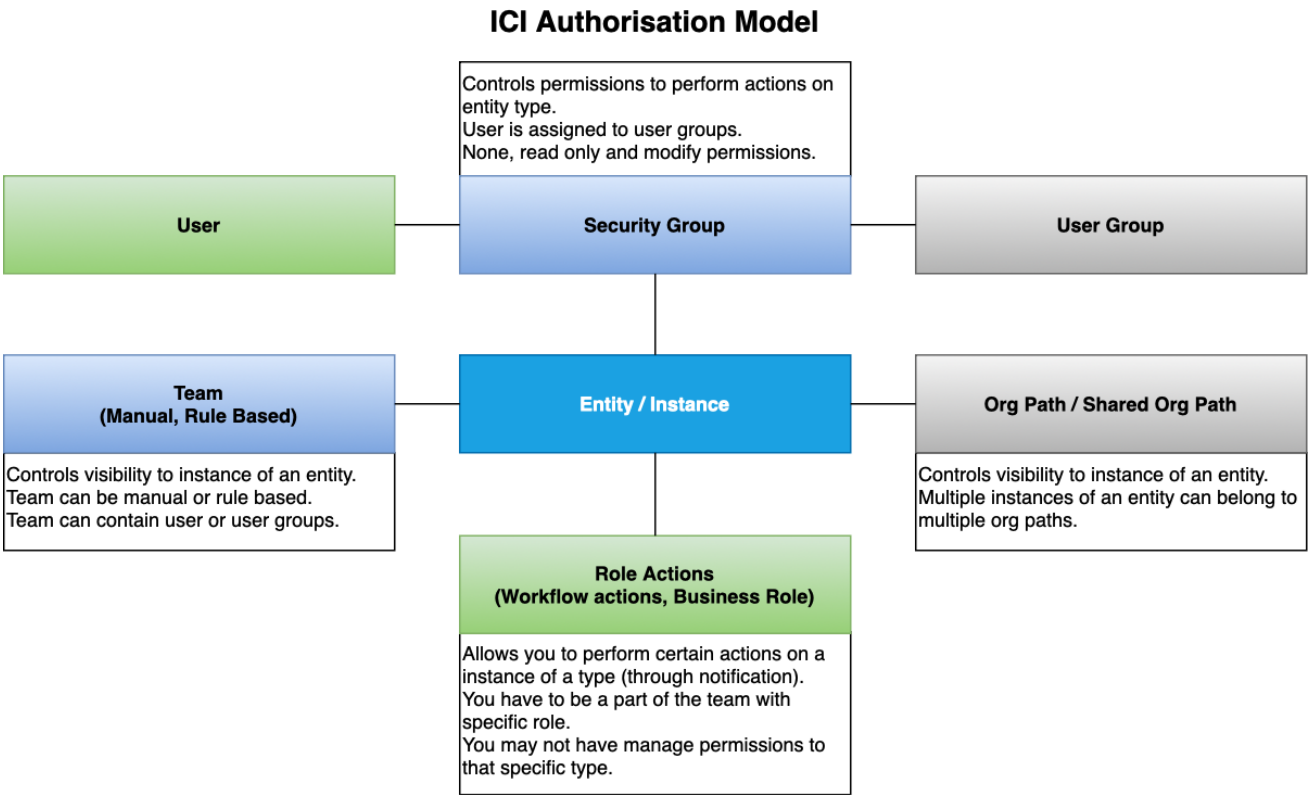
- Development: https://syensqo-dev.icertis.com/
- Test: https://syensqo-uat.icertis.com/
- Production: https://syensqo.icertis.com/

Authentication

Icertis is configured to perform SAML SSO with Syensqo Entra ID. The use of SSO is mandatorily enforced via configuration, and users cannot bypass SSO to log in with a password.

Authorization

ICertis Contract Intelligence (ICI) Authorizations are based on Security groups & role–action mapping govern feature/data access; groups are the primary container (iciwikiapac.icertis.com) .



Every Syensqo user will be assigned a position in the organization at that node of the hierarchy, or at nodes below that node. Syensqo can configure region-specific Org Units.

Authorizations in ICertis will be driven by Org structure, Security Groups configured by Syensqo.

All data and all contract documents will be stored in same deployed region, but users will access it based on their permission assigned. For example, China users will have access to only those contracts which are under “China Org”, However US Legal can have access to contracts for US as well as China.

Communication Security

- For data in transit encryption, communication is secured using SSL/TLS (TLS 1.2+) encryption, and weak ciphers are disabled.

Data Security

- Uses TLS/HTTPS for communication and AES encryption for stored data. Supports double encryption and customer-managed keys (CMK) via Azure Key Vault.
- Maintains ISO 27001, SOC 1/2, PCI DSS, HIPAA, and GDPR certifications through cloud provider (Azure) and internal policies.
- For data at rest encryption, features provided by underlying Azure services are used, e.g., TDE for SQL DB, SSE for BLOB storage, and so on. Industry-standard algorithms like AES 256 bit are used for encryption. Icertis leverages Azure’s certifications—ISO 270xx, SOC2, NIST, FedRAMP, EU Data Boundary—for regulated workloads.

Other Controls

- Icertis will provide 99.5% System Availability SLA.
- The ICI Platform is hosted on the Microsoft Azure cloud. For Azure data center compliance, please refer to https://azure.microsoft.com/en-in/overview/trusted-cloud/
- Icertis is an ISO 27001, ISO 27017, and 27018 certified organization. Icertis also complies with ITAR and has SOC2 (Type1, type2) certifications.
- Icertis Contract Intelligence platform (ICI), is hosted primarily on the Microsoft Azure cloud, where Icertis owns the cloud subscription.
- The Icertis Trust Center is a resource provided by Icertis to help customers understand the company’s commitment to security, privacy, compliance, and transparency in its cloud services and products.
- Icertis implements the following industry-standard information security frameworks to assure data confidentiality, integrity, availability, and privacy:

Sr. No	Compliance Program	Status
1	ISO 27001:2013 + ISO 27017 + ISO 27018	✓
3	SOC 1 Type II	✓
4	SOC 2 Type II + HIPAA + CCM Control Mapping	✓
5	Cyber Essentials	✓
6	ITAR	✓
7	FedRAMP	FedRAMP Ready
8	GDPR	Implemented
9	TISAX	✓

Note: FedRamp compliance only required for US Gov tenants if confirmed via a separate KDD that Icertis will be used for Release 3.

Operation Architecture

Change and Configuration Management

Please refer to document DD-TEC-170 Transport Management for Release 4.

Monitoring

- All Icertis internal critical servers and systems are configured to log general activities. This includes auditing of events on critical Windows systems such as successful logons, unsuccessful logons, access file rights successes or failures, privilege modifications, etc. The logs are maintained in the Centralized Syslog Server for 90 days.
- Event logs generated by ICI platform are stored for up to 30 days. Security event logs captured from Azure infrastructure are maintained in Microsoft Sentinel SIEM for up to 90 days.
- Icertis has implemented 'Microsoft Defender for Cloud' for security management and threat protection of user entity instances on the Microsoft Azure platform.
- A Microsoft system monitoring tool is utilized to identify availability issues or concerns with metrics such as server load alert, SQL Database Transaction Unit (DTU) utilization, failed Azure activity logs, free disk space, high disk utilization, etc. through alerts. Alerts are configured by the Icertis Cloud Operations team for each user entity instance on the Microsoft Azure platform. The Cloud Operations team receives email alerts for any breach in utilization threshold. The Cloud Operations team analyzes the alerts and if necessary, raises an incident ticket within the Freshdesk/ ServiceNow ticketing tool and takes corrective actions.
- All application-level logs are stored in the Azure SQL database, and they are encrypted at rest using TDE.

High Availability & Disaster Recovery

Icertis is deployed across multiple Azure availability zones with the following SLA:

- RPO - 24h
- RTO - 8h

Backup/Restore

- For customer data, Incremental backup is performed every 24 hours. Full back-up is performed once a week during a pre-defined maintenance window. Backups are stored on geo-replicated Azure storage.
- Ad Hoc backups are available by contacting the Icertis IT team.

Maintenance Plan

- Icertis Releases.
  - Icertis releases two major versions of Icertis Contract Intelligence every year. The major releases are typically scheduled for June and December. In between these major releases, maintenance packs are typically delivered every 4 to 6 weeks.
- Upgrade Calendar.
  - The current Upgrade calendar for major releases and maintenance packs can be accessed from the Icertis support portal. The calendar is typically updated every 6 months and provides visibility for the next 12 months. Single tenant subscribers may deviate from this calendar by scheduling their Upgrade directly with Icertis within the supported timeframe.
- Upgrade Cadence.
  - Multi-tenant subscribers are automatically Upgraded to the latest release, maintenance pack or hotfix as per the Upgrade calendar. For multi-tenant subscribers, Icertis offers a contingency opt-out from the Upgrade calendar that allows a subscriber to skip an Upgrade cycle once every two major releases (approximately once a year). Any compliant opt-out must be requested through a support ticket at least 2 weeks prior to the applicable scheduled Upgrade as mentioned in the published calendar. If there is an opt-out for an Upgrade cycle, the subscriber will automatically get Upgraded in the next cycle and does not get an option of consecutive opt-out.

Product Support

The support levels offered by ICertis are shown below. Syensqo has subscribed to the Standard support level.

Support Service & Levels

Icertis will provide the applicable Support Services within the scope, access and availability parameters set forth below.

Support Service	Standard	Gold	Platinum
Support Hours and Availability	24x5 (the work week within Subscriber's local time zone)	24x7	24x7
Support Team Engagement Model	General Support	Named Support	Named Support and Platinum Support Champion
Number of Authorized Support Contacts	2	6	9
Ticket Support Interface	Support Portal + Email	Support Portal + Email	Support Portal + Email + Phone
Customer Support Reviews	Not Applicable	Quarterly	Monthly
Request Ticket Support	Not Applicable	Up to 5 per month	Up to 10 per month

Exceptions

See also

File	Modified
File Icertis-1764339081614 draw.io diagram	Apr 27, 2026 by WENNINGER-ext, Sascha
File ~Icertis-1764339081614.tmp draw.io Draft	Apr 27, 2026 by WENNINGER-ext, Sascha
PDF File Approval by Frank Bolata 2025-12-18.pdf	Dec 18, 2025 by WENNINGER-ext, Sascha
PDF File Stakeholder endorsement - Francois Ruffinoni and Ines Narciso.pdf	Dec 08, 2025 by WENNINGER-ext, Sascha
File ~Untitled Diagram-1763489052654.tmp draw.io Draft	Nov 26, 2025 by CABELLO MARTOS-ext, Gabino
File Untitled Diagram-1763489052654 draw.io diagram	Nov 18, 2025 by CABELLO MARTOS-ext, Gabino
File ~Untitled Diagram-1763488941437.tmp draw.io Draft	Nov 18, 2025 by CABELLO MARTOS-ext, Gabino

Download All

Change log

Version	Published	Changed By	Comment
CURRENT (v. 18)	**Apr 27, 2026 12:47**	**WENNINGER-ext, Sascha**	inserted mention that use in R3 is subject to a KDD.
v. 17	Dec 10, 2025 10:02	**WENNINGER-ext, Sascha**	inserted mention that use in R3 is subject to a KDD.
v. 16	Dec 08, 2025 17:12	**WENNINGER-ext, Sascha**	added stakeholders

v. 15	Dec 02, 2025 12:55	**WENNINGER-ext, Sascha**
v. 14	Nov 28, 2025 15:45	**CABELLO MARTOS-ext, Gabino**
v. 13	Nov 28, 2025 15:36	**CABELLO MARTOS-ext, Gabino**
v. 12	Nov 28, 2025 15:20	**CABELLO MARTOS-ext, Gabino**
v. 11	Nov 28, 2025 15:11	**CABELLO MARTOS-ext, Gabino**
v. 10	Nov 25, 2025 22:41	**CABELLO MARTOS-ext, Gabino**
v. 9	Nov 25, 2025 22:28	**CABELLO MARTOS-ext, Gabino**

Go to Page History

Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

Apr 27, 2026	Actor	Type	Activity	Version
Approved	WENNINGER-ext, Sascha	State	changed state to Approved at 12:47 pm	v18
Edited following Approval	WENNINGER-ext, Sascha	State	gave *Minor change* approval at 12:47 pm *Updated to remove US-based S/4HANA system*	
		State	changed state to Edited following Approval at 12:47 pm	v18
Approved	WENNINGER-ext, Sascha	Edit	updated the page at 12:47 pm *inserted mention that use in R3 is subject to a KDD.*	
Dec 18, 2025				
	WENNINGER-ext, Sascha	State	changed state to Approved at 2:46 am	v17
Pending SteerCo Review	WENNINGER-ext, Sascha	State	gave *Final Approval* approval at 2:46 am *Approved by Frank Bolata. Email attached.*	