SYMBEEO

PUBLIC

SOLUTION DESIGN DOCUMENT

# Application platform, API and event layer, observability and workplace design for a typical buyer, applying SRA-DIG-001

Design document (HLD + LLD)

| CAPABILITY | DOCUMENT | VERSION | DATE |
|---|---|---|---|
| Digital | SDD-DIG-001 | 1.1 | Oct 10, 2026 |

WRITTEN BY

**Avinash Dhinakaran**, Principal Integration Architect



© 2026 Symbeeo. All rights reserved.

**What this document is.** The reference architecture says what a good digital platform looks like. This document is that platform applied to one client, with names, versions, routes, topics and a cut-over plan. The client here is the typical buyer from SRA-DIG-001 §1 [A]; every value marked [A] is replaced by the real client's during the design workshop. Standards and release facts carry SRA-DIG-001's source numbers (S1–S20), read Sep 24, 2026. Where a component is chosen in the buyer's comparison, this document names the slot and the test it must pass, not the product. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

## Document control

| | | | |
|---|---|---|---|
| Document | SDD-DIG-001 | Version | 1.1 |
| Issued | Oct 10, 2026 | Status | Issued by Symbeeo |
| Classification | Public | Supersedes | 1.0, Sep 27, 2026 |
| Capability | Digital | Author | Avinash Dhinakaran |
| Role | Principal Integration Architect | Applies to | SRA-DIG-001 v1.0 |
| Tested by | STP-DIG-001 | | |
| Credentials | iSAQB Certified Professional for Software Architecture – Advanced Level (CPSA-A), Oracle Certified Consultant – Value Chain Planning, Master Data Management, SCM Cloud | | |
| Approval | Approved by Edwin Ozer, Founder, Oct 10, 2026. Issued by Symbeeo, Oct 10, 2026. | | |
| Sign-off | "The customer's named representative signs this document before build; the practice lead signs it after." | | |

## Contents

1 · Introduction 3
2 · Prerequisites (all must be true before build) 4
3 · Solution overview 4
4 · Logical design 5
5 · Deployment design 6
6 · Platform services 6
7 · Migration and cut-over 6
8 · Roles and deliverables 7

© 2026 Symbeeo. All rights reserved. · Public

**Table 1.** Revision history

| Date | Version | Change |
|---|---|---|
| Sep 27, 2026 | 1.0 | First issue. |
| Oct 10, 2026 | 1.1 | Approval line now reads: approved by the Founder, issued by Symbeeo. Avinash Dhinakaran remains the author. |

# 1 · Introduction

### 1.1 Purpose.

Technical design for moving the client's application platform, API edge, event layer, telemetry and collaboration identity onto the architecture in SRA-DIG-001. After review, the client's representatives sign and work continues to build.

### 1.2 Goals.

Off every component past its support date (R8, R16); every API behind a contract and a token (R2, R3); one trace per request across edge, service and broker (R11); leavers cut in five minutes from every collaboration service that receives CAEP events, and in fifteen from any other (R15).

### 1.3 Approach and phases.

Phase 1 telemetry first, so every later change is measured. Phase 2 platform upgrade and ingress-nginx replacement. Phase 3 API contracts and edge policy. Phase 4 event layer. Phase 5 workplace: provisioning, revocation, mail, devices. Phase 6 decommission and as-built.

### 1.4 Change control.

Once this document is signed, any change to it is a **written change order** stating what changes, why, and its cost and schedule effect, signed by both parties before it is built. A signed change order is then carried out as every production change is: a merge request to the platform repository referencing this document's section, plus a ticket in the client's change system; emergency changes are reconciled into Git within 24 hours (R9) and covered by a change order at the next weekly report (§8.2).

### 1.5 Audience.

Client platform, identity and workplace teams; application owners of the 25 API-exposing applications; Symbeeo build engineers.

### 1.6 Related documents.

SRA-DIG-001 · STP-DIG-001 · SRA-SEC-001 (identity provider, SIEM) · SRA-INT-001 (ERP exchange) · SDD-NET-001 (network underneath).

© 2026 Symbeeo. All rights reserved. · Public

# 2 · Prerequisites (all must be true before build)

**Table 2.** Prerequisites (all must be true before build)

| # | Prerequisite | Owner | Status |
|---|---|---|---|
| P1 | Application inventory: 60 applications with owner, tier and interfaces | client | open |
| P2 | Identity provider confirmed able to act as OIDC issuer, SCIM client and CAEP transmitter | client | open |
| P3 | Buyer's comparison concluded for three slots: Gateway API implementation, observability backend, collaboration suite | both | open |
| P4 | Cluster capacity allocated per SRA-DC-001, on premises and in the hyperscaler | client | open |
| P5 | DNS zones delegated and certificate issuer reachable from every cluster | client | open |
| P6 | Server, endpoint and room-device inventory with OS and firmware versions | client | open |
| P7 | SLO targets agreed for each tier-1 service | client | open |
| P8 | Mail decision recorded: Exchange Server SE on premises or the vendor's online service **[S19]** | client | open |

# 3 · Solution overview

## 3.1 Architecture.

As SRA-DIG-001 §3, Figure 1.

## 3.2 Platform inventory [A].

**Table 3.** Platform inventory [A]

| Component | Placement | Count | Naming |
|---|---|---|---|
| Kubernetes production clusters | DC-A on premises; hyperscaler region | 2 | k8s-prd-dca, k8s-prd-cld |
| Kubernetes non-production | DC-B; hyperscaler | 2 | k8s-npd-dcb, k8s-npd-cld |
| Gateway API edge (slot P3) | each cluster | 3 replicas | gw-<cluster> |
| API catalog | k8s-prd-dca | 1 | api-catalog |
| Event brokers, Kafka 4.x, KRaft | k8s-prd-dca, separate node pool | 3 brokers + 3 controllers | kfk-prd-01…06 |
| OTel Collector agent | every node | 1 per node | otel-agent |
| OTel Collector gateway | each cluster | 3 | otel-gw-<cluster> |
| Metrics, traces, logs stores (slot P3) | per comparison | — | obs-* |
| SCIM and CAEP connectors | identity provider | 1 per collaboration service | idp-scim-<svc>, idp-caep-<svc> |
| Meeting-room systems | HQ and branches | 30 | room-<site>-<nn> |

© 2026 Symbeeo. All rights reserved. · Public

# 4 · Logical design

### 4.1 Environments.

Sandbox (per engineer, disposable) → non-production → production. Every environment is declared in Git; production reconciles from the `main` branch only; drift alarm at 15 minutes (R9).

### 4.2 Edge and routing.

One GatewayClass for the chosen implementation. The platform team owns one Gateway per cluster; application teams attach HTTPRoutes through ListenerSets, and cross-namespace references are allowed only by ReferenceGrant — all Standard channel since Gateway API v1.5 **[S4]**. TLS terminates at the Gateway; client-certificate validation on the partner listener **[S4]**. TCP and UDP routes, where needed, use the Standard TCPRoute and UDPRoute of v1.6 **[S4]**.

### 4.3 API policy.

Merge gate: no route merges unless its OpenAPI 3.2.0 or AsyncAPI 3.1.0 contract is in the catalog (R2) **[S5]** **[S6]**. Edge policy per route: token issuer and audience checked; authorization code with PKCE for people, client credentials for services; implicit and password grants refused (R3) **[S7]**; rate limit 50 requests/s per client [A]. AI-agent access goes through the same edge; MCP servers are registered as APIs **[S10]**.

### 4.4 Events.

Topic names `<domain>.<entity>.<event>.v<n>` [A]. Replication factor 3, min in-sync replicas 2, producer `acks=all` (R6). Work-queue consumers use share groups, production-ready since Kafka 4.2 **[S9]**. Every topic has an AsyncAPI 3.1.0 document in the catalog.

### 4.5 Identity and tokens.

People: OIDC to the client's identity provider (SRA-SEC-001). Services: client credentials, access-token lifetime 10 minutes [A]. Collaboration services: SCIM 2.0 provisioning, joiner and mover ≤ 15 minutes (R14) **[S16]**; CAEP session-revoked and credential-change events on disable (R15) **[S15]**.

### 4.6 Telemetry pipeline.

SDKs export OTLP to the node agent; the agent adds Kubernetes resource attributes and forwards to the gateway tier; the gateway tail-samples (100 % of error and slow traces, 10 % of the rest [A]) and routes to the stores. Semantic conventions pinned to 1.44.0 **[S12]**. W3C `traceparent` propagated through the edge and carried in Kafka record headers, so a request is one trace across broker hops (R11) **[S14]**. Pipeline drop counters exported as metrics and alerted at 0.1 % (R12). Retention per R18.

### 4.7 Service-level objectives.

One availability SLO and one latency SLO per tier-1 service (values from P7); multi-window burn-rate alerts page on-call within 5 minutes (R13).

### 4.8 Workplace devices.

Windows 11 on every endpoint (Windows 10 support ended October 14, 2025 **[S18]**). Room and phone devices on a certified Android 12 or later release, certification to August 15, 2028 or later **[S17]**, or the equivalent check for the suite chosen in P3.

© 2026 Symbeeo. All rights reserved. · Public

# 5 · Deployment design

### 5.1 Repository layout.

`platform/` (clusters, Gateway, collectors, brokers), `apps/<team>/` (routes, topics, contracts), `policies/` (edge, admission). One pull request per change.

### 5.2 Software baseline [A].

Recorded at staging and in the as-built with checksums:

**Table 4.** Software baseline [A]

| Component | Baseline rule |
|---|---|
| Kubernetes | 1.36 or 1.37, latest patch **[S1]** |
| Gateway API CRDs | Standard channel, v1.5 or later **[S4]** |
| Kafka | 4.3.x, latest patch **[S9]** |
| OpenTelemetry Collector and SDKs | current release; semantic conventions 1.44.0 **[S12]** |
| eBPF instrumentation | current 0.x, coverage only, not audit evidence **[S12]** |
| Mail | per P8 **[S19]** |

### 5.3 Access.

Secrets in the client's vault; Symbeeo holds no production credentials after handover.

# 6 · Platform services

### 6.1 DNS.

One record per Gateway listener; global DNS health-checks both production clusters (SRA-DIG-001 F2). **6.2 Certificates.** Issued automatically from the client's issuer; expiry alert at 21 days (F9). **6.3 Time.** Every node on the client's NTP sources; trace timestamps depend on it. **6.4 Backup.** Cluster state is Git; control-plane datastore snapshots daily [A]; broker configuration in Git, data by replication.

# 7 · Migration and cut-over

**Table 5.** Migration and cut-over

| Step | Action | Rollback |
|---|---|---|
| 1 | Deploy OTel agents and gateways beside existing monitoring agents; dual-run two weeks | remove collectors |
| 2 | Upgrade clusters to the §5.2 baseline, one minor at a time, non-production first | restore from snapshot |
| 3 | Install the Gateway API edge beside ingress-nginx; translate each Ingress to an HTTPRoute; move DNS one application per window | DNS back to the old ingress |
| 4 | Remove ingress-nginx when zero routes remain (R8) | — |

© 2026 Symbeeo. All rights reserved. · Public

| Step | Action | Rollback |
|---|---|---|
| 5 | Edge token and contract policy in report-only mode for two weeks, then enforce | return to report-only |
| 6 | New Kafka 4.x cluster; mirror topics; move producers, then consumers | repoint to the old cluster |
| 7 | Workplace: SCIM and CAEP per service; mail per P8; replace out-of-support endpoints and room devices | old device kept one week |
| 8 | Decommission, as-built, acceptance (STP-DIG-001 §4) | — |

# 8 · Roles and deliverables

## 8.1 Roles.

**Table 6.** Roles

| Role | Symbeeo | Client |
|---|---|---|
| Design authority | practice lead (signs) | head of infrastructure (signs) |
| Build | build engineers | change approver |
| Acceptance | test lead | named acceptor |

## 8.2 Weekly status report.

Every week from signature to acceptance: % complete per deliverable (§8.5 and each phase of §1.3), slippage against the signed plan with its cause, open change orders (§1.4).

## 8.3 Escalation contacts [A].

Named at the design workshop; roles fixed here.

**Table 7.** Escalation contacts [A]

| Level | Symbeeo | Client | When |
|---|---|---|---|
| 1 | build lead | platform lead | any blocked task |
| 2 | practice lead | head of infrastructure | slippage past one week, or a disputed change order |
| 3 | Founder | CIO | unresolved at level 2 within 5 business days |

## 8.4 Security and lifecycle clauses.

- A security incident affecting the client's data or systems is **reported to the client's security contact within 24 hours** of discovery.
- Storage media leaving the client's control — replaced servers, endpoints and room devices (§7 step 7) — are **sanitized to NIST SP 800-88 Rev. 2** (Guidelines for Media Sanitization, final, September 2025; `https://csrc.nist.gov/pubs/sp/800/88/r2/final`, read Sep 24, 2026), with a certificate per device. Media may instead stay with the client under a non-return service; media holding PHI or other regulated personal data are never taken back unsanitized.

© 2026 Symbeeo. All rights reserved. · Public

- **No equipment is quoted past its vendor's end-of-sale date**, and every item's end-of-support date is shown on the quote. In this practice that covers what is supplied: servers, endpoints, room and phone devices (R16), and the software subscriptions they run.
- **Every quote states the vendor support level by severity**: response time for severity 1 to 4.

### 8.5 Handover pack.

As-built (clusters, versions, routes, topics, contracts, collectors, connectors, device list) · configurations as the Git repository at handover · credentials transferred into the client's vault, Symbeeo access removed (§5.3) · licenses and subscriptions · support contracts · operations runbook · STP-DIG-001 signed with results · sanitization certificates · open items. With this document and the acceptance certificate, these are the deliverables.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

## Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SDD-DIG-001 · Version 1.1 · Oct 10, 2026