SYMBEEO

PUBLIC

DESIGN STUDY

Open-finance API edge for a retail bank: FAPI 2.0 tokens, Gateway API, OpenShift 4.22

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Digital	Financial Services	EU retail bank
DOCUMENT	**VERSION**	**DATE**
DIG-002	1.2	Oct 10, 2026

WRITTEN BY

Avinash Dhinakaran, Principal Integration Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	DIG-002	Version	1.2
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.1, Oct 7, 2026
Capability	Digital	Industry	Financial Services
Author	Avinash Dhinakaran	Role	Principal Integration Architect
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. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the standard owner's or vendor's own current page on Sep 24, 2026 · [S*] figure from the owner's page summary where the page itself could not be opened · [A] design assumption · [T] design target (the record's outcome figure and anything derived from it). Every figure carries one tag. No figure comes from any prior engagement, file or asset. 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.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 7, 2026	1.1	One public deployment removed from §1c; no figure depended on it.
Oct 10, 2026	1.2	Approval line now reads: approved by the Founder, issued by Symbeeo. Avinash Dhinakaran remains the author.

1 · Scope

Who it is for. The head of platform engineering or the chief information security officer of a retail bank that exposes account and payment APIs to licensed third-party providers, runs them on Red Hat OpenShift clusters whose update support is running out, and must show a supervisor that every third-party call is authenticated, sender-constrained and logged.

Typical buyer [A]. A retail bank in the EU with 1.2 million customers, 14 open-finance APIs used by 40 registered third-party providers, two data centers, two OpenShift production clusters on 4.16 [A]. Peak partner load 600 requests/s [A].

What is in. Cluster update to a supported OpenShift release; the partner listener: an OpenShift passthrough Route to the API management gateway, which terminates mutual TLS, with Gateway API routing behind it; the authorization server profile for third-party access (FAPI 2.0); API contracts in a catalog; token checks at the edge; the audit trail of every partner call into the bank's SIEM. **What is out.** The authorization server product itself (the bank's identity platform, SRA-SEC-001); customer consent screens; core banking; the network under the clusters (SRA-NET-001).

Assumptions. Third-party providers present qualified certificates the bank already trusts [A]. The bank's identity platform can issue sender-constrained tokens (checked at design, §6) [A]. Both clusters stay on premises for data residency [A].

Related documents, read Sep 24, 2026. SRA-DIG-001, SDD-DIG-001, STP-DIG-001 v1.0 (issued Sep 27, 2026) · FAPI 2.0 Security Profile, Final, OpenID Foundation (`https://openid.net/specs/fapi-security-profile-2_0-final.html`) · OpenShift Container Platform 4.22 release notes (`https://docs.redhat.com/en/documentation/openshift_container_platform/4.22/html-single/release_notes/index`) · Red Hat product life cycle, OpenShift Container Platform 4 (`https://access.redhat.com/product-life-cycles/?product=OpenShift%20Container%20Platform%204`) · Gateway API v1.5 and v1.6 (`https://kubernetes.io/blog/2026/04/21/gateway-api-v1-5/` · `https://kubernetes.io/blog/2026/08/03/gateway-api-v1-6-release/`) · Kubernetes releases (`https://kubernetes.io/releases/`) · OpenShift 4.22 updating clusters, Control Plane Only update and ingress and load balancing, read Sep 27, 2026 (`https://docs.redhat.com/en/documentation/openshift_container_platform/4.22/html-single/updating_clusters/index#control-plane-only-update` · `https://docs.redhat.com/en/documentation/openshift_container_platform/4.22/html-single/ingress_and_load_balancing/index`) · Regulation (EU) 2022/2554, Digital Operational Resilience Act (`https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng`).

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Our own design, built from published documentation. OpenShift Container Platform 4.22	Red Hat · GA Jun 9, 2026; release notes read Sep 24, 2026 and Sep 27, 2026	4.22 runs Kubernetes 1.35, inside upstream support to Feb 28, 2027; its Gateway API runs on Red Hat OpenShift Service Mesh 3.3.1 and Istio 1.28.5 and vendors the Standard-channel Gateway API v1.4.1 CRDs; maintenance support to Dec 31, 2027, extended update support to Jun 30, 2028	`https://docs.redhat.com/en/documentation/openshift_container_platform/4.22/html-single/release_notes/index`
Our own design, built from published documentation. FAPI 2.0 Security Profile	OpenID Foundation · Final, February 22, 2025	The partner token rules R5–R8 are this profile's text: pushed authorization requests, PKCE with S256, sender-constrained tokens by mTLS or DPoP, authorization codes of 60 s at most	`https://openid.net/specs/fapi-security-profile-2_0-final.html`
Our own design, built from published documentation. Gateway API v1.5	Kubernetes project · April 21, 2026	Upstream, frontend client-certificate validation moved to the Standard channel in v1.5. OpenShift 4.22 vendors v1.4.1 and its Gateway reference documents no client-certificate field (read Sep 27, 2026), so §4.2 does not rely on it until OpenShift ships v1.5 or later	`https://kubernetes.io/blog/2026/04/21/gateway-api-v1-5/`

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	14 partner APIs · 40 third-party providers · 2 production clusters	[A]
R2	Platform release	OpenShift 4.22 on Kubernetes 1.35; vendor maintenance to Dec 31, 2027	[S] Red Hat
R3	Current release	OpenShift 4.16: EUS term 1 ended Jun 27, 2026; term 2 runs to Jun 27, 2027	[S] Red Hat
R4	Partner API contracts	14 of 14 in OpenAPI 3.2.0 in the catalog before the edge accepts a route	[S] SRA-DIG-001 R2
R5	Authorization requests	pushed authorization requests only; others rejected	[S] FAPI 2.0
R6	PKCE	required, S256	[S] FAPI 2.0
R7	Access tokens	sender-constrained only, by mTLS or DPoP	[S] FAPI 2.0

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R8	Authorization code lifetime	≤ 60 s	[S] FAPI 2.0
R9	Implicit and password grants	0 accepted	[S] RFC 9700 via SRA-DIG-001 R3
R10	Latency added by the edge	≤ 10 ms p95 at 600 requests/s	[T]
R11	Edge availability	99.95 % per calendar month	[T]
R12	Partner call audit	every call logged with provider ID, API, token ID, result; in the SIEM ≤ 5 min	[T]
R13	Regulation	EU Digital Operational Resilience Act applies from January 17, 2025	[S] Regulation (EU) 2022/2554, Art. 64
R14	Update window	both clusters on 4.22 by Jan 29, 2027, inside Kubernetes 1.35 upstream patch support (ends Feb 28, 2027, §4.1)	[T]

Fourteen rows; nine carry a standard's or vendor's figure, one is a design assumption, four are design targets.

3 · Architecture overview

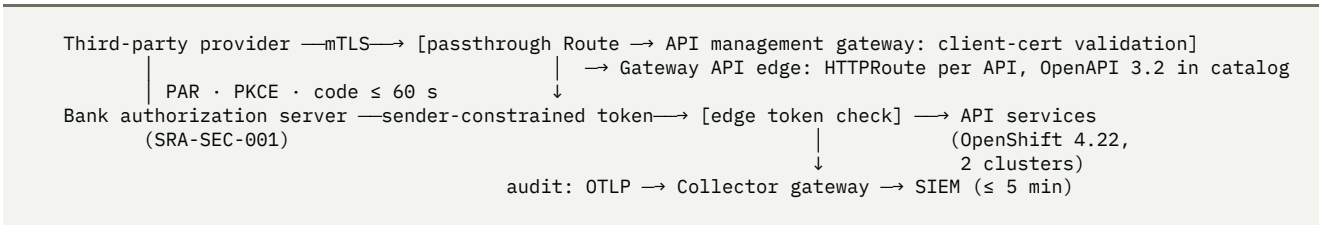


Figure 1. Partner API access path

One partner listener per cluster, one token rule set, one audit path. The parts table lists platform releases and profiles rather than hardware.

Table 4. Architecture overview

Role	Component (exact name)	Qty	Capacity used	Why this unit
Platform	OpenShift Container Platform 4.22	2 production, 2 non-production clusters	14 APIs	Kubernetes 1.35; maintenance to Dec 31, 2027 [S]
North–south edge	OpenShift Gateway API (Red Hat OpenShift Service Mesh 3.3.1, Istio 1.28.5)	1 Gateway per cluster, 3 replicas	600 requests/s peak [A]	shipped with 4.22 [S]; implementation choice [A]
Partner listener	OpenShift Route, passthrough termination, to the API management gateway, which terminates mutual TLS	1 per cluster	40 providers [A]	passthrough is Red Hat's documented way to require client certificates on a Route [S]; OpenShift 4.22's Gateway API (v1.4.1) documents no frontend client-certificate validation [S]

© 2026 Symbeeo. All rights reserved. · Public

Role	Component (exact name)	Qty	Capacity used	Why this unit
Token profile	FAPI 2.0 Security Profile, Final	1	40 client registrations [A]	the third-party access profile [S]
API contracts	OpenAPI 3.2.0 documents in the catalog	14	—	SRA-DIG-001 R2 [S]
Audit transport	OpenTelemetry Collector gateway, OTLP	3 per cluster	600 records/s [A]	SRA-DIG-001 §4.7 [S]

4 · Design by subsystem

4.1 Platform update.

Both clusters move from 4.16 to 4.22 by three Control Plane Only updates, Red Hat's current name for EUS-to-EUS updates: 4.16 → 4.18, 4.18 → 4.20, 4.20 → 4.22. In each, the worker machine config pools are paused, the control plane is updated through the odd release between (for example 4.20 → 4.21 → 4.22), and the pools are unpaused once, so workers are updated once per step rather than at each release [A]; a direct 4.y to 4.y+2 jump is not possible [S]. Non-production first [A]; each step is taken only when both releases are in the stable channel [S], checked against Red Hat's update graph at design freeze [A]. 4.22 runs Kubernetes 1.35 [S], inside upstream patch support until Feb 28, 2027 [S], so production completes by Jan 29, 2027 (R14) [T]. From Mar 1, 2027 the clusters sit outside SRA-DIG-001 R7 until the next OpenShift minor on Kubernetes 1.36 or later is installed; this is recorded as a deviation, covered by Red Hat maintenance to Dec 31, 2027 [S], and that update is planned once the release is generally available [A]. Rejected: staying on 4.16 under term 2 — it buys nine months and ends Jun 27, 2027 [S].

4.2 Partner listener.

Upstream Gateway API moved frontend client-certificate validation to the Standard channel in v1.5 [S], but OpenShift 4.22 vendors v1.4.1 and documents no such field [S]. So the partner hostname is an OpenShift Route with passthrough termination to the API management gateway (SRA-DIG-001 D3), which validates the provider's client certificate at the TLS handshake [S] Red Hat, passthrough Routes; product [A]. Behind it, one Gateway per cluster carries one HTTPRoute per API; cross-namespace references only by ReferenceGrant [S]. When an OpenShift release vendors Gateway API v1.5 or later with this validation documented, the listener moves onto the Gateway and the Route is retired [A]. The bank's existing Routes stay for staff applications [A]. Rejected: a per-API load balancer — 14 certificate configurations instead of one (R12 audit gaps).

4.3 Token rules.

The authorization server is configured to FAPI 2.0: pushed authorization requests only (R5), PKCE with S256 (R6), sender-constrained access tokens (R7), codes valid 60 s at most (R8) [S]. The bank chooses mTLS binding, because providers already hold certificates for the partner listener [A]. Implicit and password grants are refused (R9) [S].

4.4 Edge token check.

At the API management gateway, which holds the client certificate from the mutual-TLS handshake (§4.2), each call's token is checked for issuer, audience and expiry, and its certificate thumbprint compared with that certificate [A]. Rate limit 50 requests/s per provider [A].

© 2026 Symbeeo. All rights reserved. · Public

4.5 Contracts.

No HTTPRoute merges without its OpenAPI 3.2.0 document in the catalog (R4) [S]. Security tests on the five highest-traffic APIs follow the OWASP API Security Top 10, 2023 edition [S] (SRA-DIG-001 S8).

4.6 Audit.

Every partner call emits one log record over OTLP with provider ID, API, token ID and result; the Collector gateway forwards to the bank's SIEM, target ≤ 5 min (R12) [T]. Record size 1 kB at 600 requests/s peak: about 2 GB an hour at peak [A].

4.7 Timeline.

Non-production on 4.22 by Dec 18, 2026, production by Jan 29, 2027 (R14) [T]; partner listener cut over provider by provider in the two weeks after [A].

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
One edge replica down	remaining replicas serve; no partner-visible error beyond retries	[A]
Edge tier down in one cluster	global DNS moves partner traffic to the other cluster ≤ 60 s	[A] SRA-DIG-001 F2
Provider certificate revoked	TLS handshake refused at the partner listener; logged	[A]
Token without a certificate binding	call refused at the edge; logged as a policy failure	[S] FAPI 2.0; [A]
Authorization server unreachable	new authorizations fail; issued tokens honored to expiry; no fail-open	[A] SRA-DIG-001 F6
SIEM unreachable	Collector buffers to its disk limit; drops counted and alerted	[A]

6 · Limits

- Kubernetes 1.35 leaves upstream patch support on Feb 28, 2027 [S]; after that the cluster relies on Red Hat maintenance to Dec 31, 2027 [S] and is a recorded deviation from SRA-DIG-001 R7 until the next OpenShift minor is installed (§4.1).
- FAPI 2.0 support in the bank's authorization server is an assumption until the design workshop confirms it; if it fails R5–R8, the identity platform is re-compared, not the edge.
- OpenShift 4.22 documents no Gateway API frontend client-certificate validation (read Sep 27, 2026), so the partner listener is a passthrough Route to the API management gateway until a later OpenShift release documents it.
- No figure here has been measured; every latency, rate and date is an assumption or a target.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

8 · The author

WRITTEN BY

Avinash Dhinakaran

Principal Integration Architect

iSAQB Certified Professional for Software Architecture – Advanced Level (CPSA-A), Oracle Certified Consultant – Value Chain Planning, Master Data Management, SCM Cloud

Signed off by Edwin Ozer, Founder.

© 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.

DIG-002 · Version 1.2 · Oct 10, 2026