Kerangka Acuan Kerja

API Management – Phase 1

PT Kliring Berjangka Indonesia (Persero)

07/09/2026

DIVISI TEKNOLOGI INFORMASI

PT KLIRING BERJANGKA INDONESIA (Persero)

Menara Danareksa Lt. 6

Jl. Medan Merdeka Selatan No. 14, Gambir

Jakarta Pusat, DKI Jakarta 10110

Tel. 021-35280000

Fax. 021-35282000

Kerangka Acuan Kerja

Pembangunan API Management Platform (Core Foundation)

Nama Inisiatif	Pembangunan API Management Platform – Fase 1 (Core Foundation)
Versi Dokumen	1.0
Tanggal	03 September 2026
Status	Final
Pemilik Dokumen	Divisi Teknologi Informasi
Phase	1

Lembar Pengesahan

Prepared By	 Reza Fachrizal Adnan (Teknologi Informasi Specialist)	date : 07/09 2026
Reviewed By	 Roeswan Roesli (Kepala Divisi Operasional & Pengembangan Bisnis PBK)	date : 07/09 2026
Approved By	 Oki Marsetiawan (Kepala Divisi Teknologi Informasi)	date : 07/09 2026

Daftar Isi

1. Latar Belakang

Integrasi sistem antar unit kerja internal, entitas anak, mitra bisnis (B2B), dan regulator menuntut pertukaran data yang cepat, aman, dan terstandarisasi. Ketiadaan gerbang integrasi terpusat saat ini menimbulkan fragmentasi keamanan (*point-to-point integration*), keterbatasan visibilitas audit trafik, potensi penurunan performa backend akibat lonjakan beban (*traffic spike*), serta inefisiensi proses integrasi mitra.

Guna menjawab tantangan tersebut, diperlukan pelaksanaan **Fase 1: Core Foundation Setup** untuk membangun platform API Management terpusat (*enterprise-grade*) yang berfungsi sebagai pintu gerbang tunggal (*single point of entry*), mengelola otorisasi terpusat, memitigasi ancaman keamanan siber, dan menyediakan katalog mandiri (*self-service*) bagi para pengembang.

2. Tujuan

Dokumen ini mendefinisikan kebutuhan bisnis, fungsional, non-fungsional, dan arsitektural yang menjadi dasar pelaksanaan Fase 1 – Pembangunan Fondasi Platform API Management (Core Foundation). Dokumen ini digunakan sebagai acuan utama bagi Tim Enterprise Architecture, Rekayasa Perangkat Lunak, Infrastruktur On-Premise, Information Security (InfoSec), serta Vendor Penyedia Solusi dalam melaksanakan perencanaan, perancangan, implementasi, pengujian, hingga kesiapan operasional platform API Management.

Pelaksanaan Fase 1 bertujuan untuk membangun fondasi API Management yang terintegrasi, aman, tersedia secara high availability, terukur, serta dapat dikelola secara terpusat, sebagai dasar bagi pengembangan dan perluasan ekosistem API pada fase selanjutnya.

Adapun tujuan utama yang ingin dicapai dalam Fase 1 meliputi:

1. **Membangun dan mengonfigurasi API Gateway Core** sebagai *centralized gateway* untuk mengelola dan mengendalikan trafik API antara konsumen API dengan sistem backend.
2. **Menyediakan dan mengintegrasikan Identity and Access Management (IAM)/OAuth2 Server** untuk mendukung mekanisme autentikasi, otorisasi, pengelolaan identitas aplikasi, serta pengendalian akses terhadap API.
3. **Menyediakan Developer Portal dan API Catalog berbasis self-service** untuk mendukung proses registrasi developer/application, publikasi dokumentasi API, pengajuan akses atau subscription, serta pengelolaan API secara terstruktur.
4. **Menerapkan kebijakan keamanan trafik API** yang mencakup *rate limiting*, WAF, IP filtering, payload validation, dan *threat protection* untuk melindungi API dan sistem backend dari penyalahgunaan maupun ancaman keamanan.
5. **Menyediakan infrastruktur High Availability (HA) dan Load Balancer** untuk memastikan ketersediaan layanan API Gateway, mendukung mekanisme failover, serta memungkinkan peningkatan kapasitas secara horizontal sesuai kebutuhan.
6. **Menyediakan kemampuan monitoring, logging, tracing, dan analytics secara terpusat** untuk memberikan visibilitas terhadap performa, trafik, keamanan, dan kondisi operasional API Management serta mendukung proses monitoring dan troubleshooting.

7. **Menerapkan standardisasi dokumentasi dan tata kelola API (API Governance)**, termasuk penggunaan standar OpenAPI 3.0, API versioning, lifecycle management, change management, serta pengelolaan API Catalog.
8. **Melaksanakan Initial Security Assessment dan Penetration Test terhadap platform** untuk mengidentifikasi potensi kerentanan keamanan pada komponen API Management sebelum digunakan pada lingkungan produksi, termasuk proses remediasi dan pengujian ulang atas temuan yang relevan.
9. **Menyiapkan dokumentasi teknis dan operasional serta knowledge transfer** kepada tim terkait guna memastikan kesiapan pengelolaan, pemeliharaan, monitoring, troubleshooting, dan pengoperasian platform API Management setelah implementasi selesai.

3. Sasaran

Sasaran	Target/Baseline
Availability	Uptime minimal 99,9%
Performance	Gateway processing overhead maksimum 5 ms p95 untuk request standar
Throughput	Minimum 1.500 RPS/TPS sesuai skenario pengujian
Security	Zero Critical dan Zero High sebelum production
Transport	TLS 1.3
API Standard	100% OpenAPI 3.0 + automated linting
HA	Gateway cluster/load balancing; minimal dua Availability Zones sesuai target architecture
Scalability	Horizontal scaling/HPA sesuai desain platform

4. Ruang Lingkup dan Batasan

4.1. Ruang Lingkup

Ruang lingkup inisiatif mencakup sembilan komponen utama berikut:

1. Setup dan konfigurasi API Gateway Core;
2. Lisensi dan subscription platform API Management untuk tahun pertama;
3. Developer Portal dan API Catalog berbasis self-service;
4. Identity and Access Management (IAM) / OAuth2 Server;
5. Kebijakan keamanan trafik, termasuk rate limiting, WAF, dan threat protection;
6. Dashboard monitoring, logging, dan analitik terpusat;
7. Standarisasi API documentation dan tata kelola governance;
8. Infrastruktur High Availability (HA) dan Load Balancer;
9. Initial Security Assessment / Penetration Test Platform.

4.2. Batasan

KAK ini secara khusus berlaku untuk Fase 1 – Core Foudation. Fase lanjutan bukan kewajiban penyedia kecuali disepakati melalui perubahan ruang lingkup.

1. Tidak termasuk penggantian/modernisasi business logic backend;
2. Tidak termasuk full API ecosystem lanjutan;
3. Tidak termasuk monetization / billing penuh;
4. Tidak termasuk fitur Fase 2 dan seterusnya;
5. Pengerjaan Hanya dalam ruang lingkup Fase 1;

5. Hasil yang diharapkan

5.1. Expected Business Outcome

1. Platform terpasang dan terkonfigurasi
2. Gateway runtime berjalan HA
3. IAM/outh2 terintegrasi
4. Developer Portal/API Catalog tersedia
5. Security policy baseline diterapkan
6. Observability terpusat tersedia
7. API Governance / OpenAPI baseline tersedia
8. Testing dan security Assessment terdokumentasi
9. Knowledge transfer dan operational documentation tersedia

5.2. Physical /Digital Deliverable

No	Deliverable	Minimum Content
1	Project Charter & Project Plan	Scope, objective, stakeholder, schedule, risk/dependency
2	Solution Architecture	HLD, components, integration, deployment
3	Security Architecture	Security layer, flow, trust boundary, controls
4	API Inventory/Catalog	Metadata, owner, version, documentation
5	OpenAPI Specification	OpenAPI 3.0 specification
6	Configuration Baseline	Gateway, route, upstream, policy, environment
7	Developer Portal	Catalog, registration, subscription/access
8	IAM Integration	OAuth2/OIDC, JWT, client/access configuration
9	Observability Dashboard	Metrics, logs, traces, alerts, audit
10	SIT Report	Functional/integration result
11	Performance Report	Throughput, latency, scenario
12	HA/Failover Report	Health check, node failure/failover result
13	VAPT Report	Finding, severity, remediation, retest
14	UAT Report	Scenario, result, evidence, sign-off
15	Runbook	Operation, incident, backup/restore, deployment, troubleshooting
16	As-Built Document	Final architecture and implemented configuration
17	Knowledge Transfer	Material and evidence
18	Final Report	Implementation summary, issue/status, recommendation

6. Arsitektur

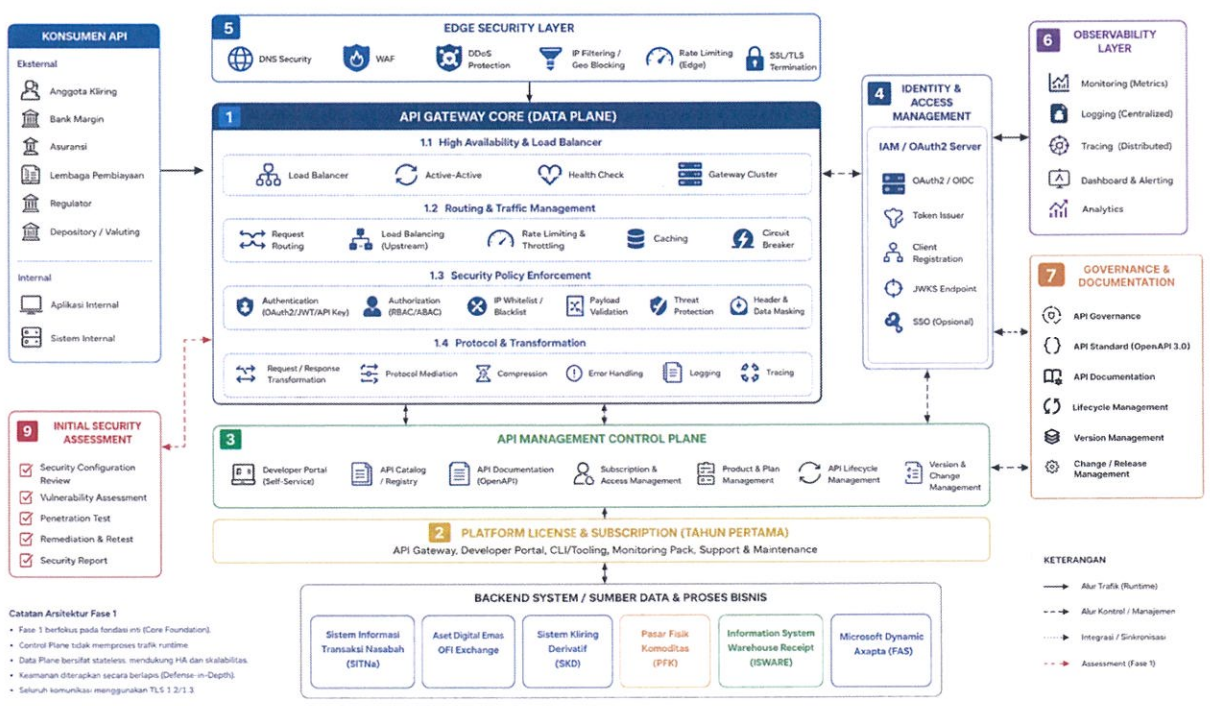
6.1. Prinsip Arsitektur

Keenam prinsip arsitektur tersebut menjadi baseline desain dan implementasi API Management Fase 1. Penyedia wajib memastikan bahwa solusi yang ditawarkan dan diimplementasikan memenuhi prinsip sebagai berikut:

- **Decoupled Architecture:** Pemisahan antara Control Plane sebagai bidang manajemen konfigurasi dan Data Plane sebagai bidang pemrosesan trafik.
- **Stateless Processing:** Instance Data Plane bersifat stateless untuk mempermudah auto-scaling dan distribusi beban yang merata.
- **Defense-in-Depth:** Penerapan lapisan keamanan bertingkat mulai dari Edge Load Balancer, WAF, API Gateway Policy, hingga autentikasi token.
- **Configuration-as-Code:** Seluruh konfigurasi rute, upstream, dan plugin didefinisikan secara deklaratif dan dikelola melalui kontrol versi Git.

Setiap penyimpangan terhadap prinsip tersebut wajib dijelaskan dalam dokumen desain dan memperoleh persetujuan dari pihak yang berwenang sebelum implementasi dilakukan.

6.2. Arsitektur Target



Gambar 1 Arsitektur API Management Platform – FASE 1 (Core Foundation)

Catatan Arsitektur Fase 1

1. **Core Foundation**

   Implementasi Fase 1 difokuskan pada Pembangunan fondasi utama API Management yang mencakup API Gateway, IAM/OAuth, Developer Portal, API Catalog, Keamanan trafik, Observability, Governance, serta Infrastruktur HA.

2. **Pemisahan Control Plane dan Data Plane**

   Control Plane digunakan untuk fungsi Administrasi, Konfigurasi, Lifecycle management, API catalog, Subscriptiom, dan Governance, seluruh trafik API runtime diproses oleh Data Plane/ API Gateway

3. **Stateless Data Plane**

   Data Plane dirancang bersifat stateless sehingga node API Gateway dapat bekerja secara redundant, mendukung High Availability, Failover, dan Horizontal Scaling

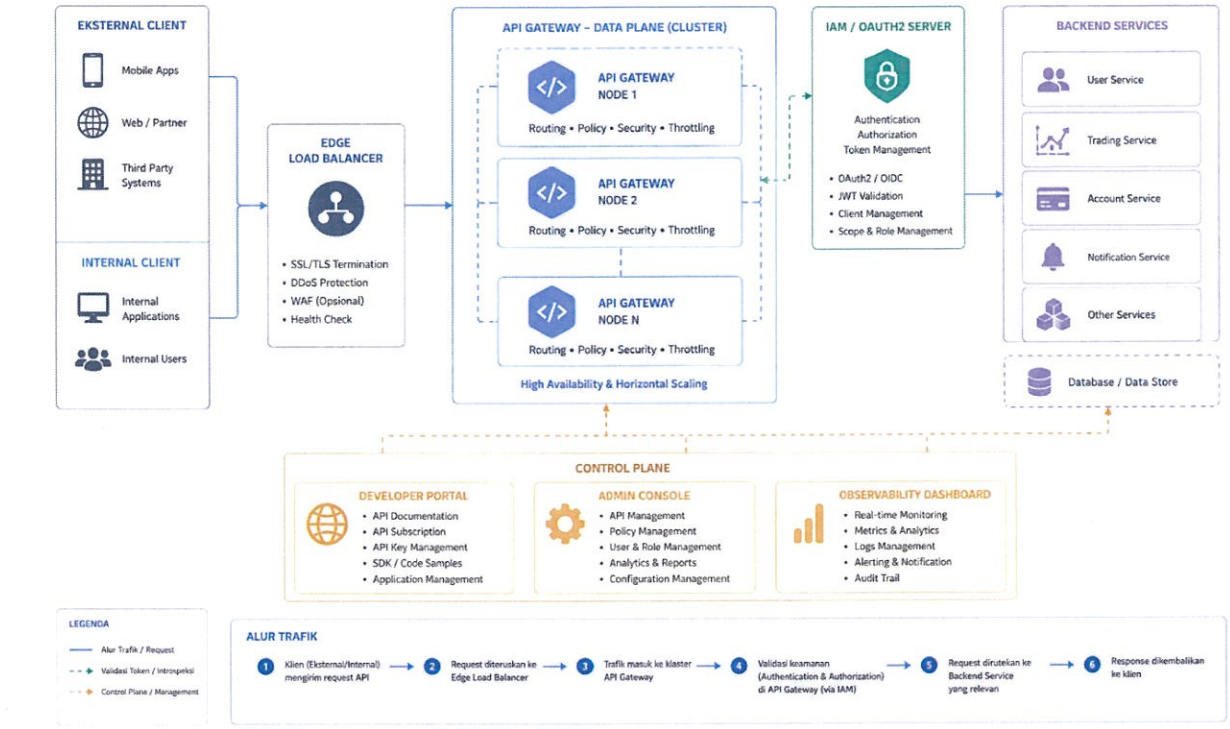
4. **Defense-in-depth**

   Keamanan diterapkan secara berlapis mulai dari Perimeter/Edge Security, WAF, IP filtering, TLS, Authentication & authorization, Rate Limiting, Payload Validation, hingga Treat Protection.

5. **Secure Communication**

   Komunikasi antara client, API Gateway, IAM, dan backend menggunakan TLS 1.3 sesuai kebijakan keamanan organisasi

6.3. Topologi Arsitektur



Gambar 2 Topologi Arsitektur API Management – FASE 1

Topologi Fase 1 terdiri dari :

1. klien internal/eksternal,
2. edge load balancer,
3. cluster Data Plane,
4. IAM/OAuth2,
5. backend services,
6. serta Control Plane dengan Developer Portal,
7. Admin Console dan Observability Dashboard

7. Kebutuhan Functional

ID Kebutuhan	Modul / Komponen	Deskripsi Kebutuhan Fungsional
FR-01	Routing & Proxy Engine	Sistem harus mampu melakukan dynamic routing berbasis path URI, HTTP method, header, dan query parameter ke upstream backend yang sesuai tanpa restart service.
FR-02	Manajemen Upstream & Failover	Gateway wajib mendukung load balancing upstream dan circuit breaker otomatis jika backend mengalami kegagalan.
FR-03	Autentikasi & Otorisasi	Gateway harus memvalidasi token JWT secara lokal berbasis public key dan mendukung grant OAuth2 utama.
FR-04	Self-Service Developer Portal	Portal harus menyediakan pendaftaran akun developer, pembuatan aplikasi, rotasi kredensial, dan manajemen redirect URI.
FR-05	API Catalog & Mocking	Portal wajib menampilkan katalog API interaktif dengan kapabilitas uji coba langsung menggunakan mock data.
FR-06	Workflow Persetujuan Akses	Portal harus memiliki alur approval berjenjang untuk akses ke scope API privat atau sensitif.
FR-07	Kebijakan Rate Limiting	Sistem harus membatasi laju request berdasarkan IP Address, Client ID, dan Tier API.
FR-08	Payload Inspection & WAF	Gateway harus memblokir request di atas batas payload dan mendeteksi pola injeksi seperti SQLi dan XSS.
FR-09	Log Masking & Audit Trail	Seluruh akses API harus dicatat dalam log terstruktur dengan masking otomatis pada field sensitif.
FR-10	Metrics & Alerting	Sistem harus mengumpulkan metrik RED dan memicu alert saat error rate HTTP 5xx melebihi ambang batas.
FR-11	Flexible & Dinamis	Sistem harus flexible dan dapat di redevelop dan reconfigurasi jika terdapat penambahan dan perubahan dalam proses bisnis

8. Kebutuhan Non- Fungsional

Kategori	Requirement	Target / Acceptance
Performance	Gateway overhead	Overhead pemrosesan API Gateway tidak boleh melebihi 5 ms pada percentile ke-95 (p95) untuk request API standar, tidak termasuk latency jaringan dan waktu pemrosesan pada backend
Throughput	Baseline capacity	Platform API Management harus mampu menangani throughput minimal 1.500 RPS pada skenario beban puncak (peak load) yang telah ditetapkan, dengan tetap memenuhi parameter performa dan SLA yang disepakati
Availability	Platform availability	≥ 99,9% SLA
HA	No single gateway node dependency	Minimal dua node yang ditempatkan pada infrastruktur/site yang berbeda sesuai dengan final architecture design.
Deployment	Update configuration/patch	Zero-downtime sesuai desain
Scalability	Data Plane scaling	Horizontal scaling/ autoscaling
Security	Transport	TLS 1.3
VAPT	Pre-production security	Zero Critical & Zero High
Governance	API specification	100% OpenAPI 3.0 + automated linting
Logging	Structured + masking	Coverage sesuai API production scope
Traceability	Correlation/trace ID	End-to-end trace sesuai kemampuan platform

Keterangan :

- **Skalabilitas:** Data Plane wajib mendukung Horizontal Pod Autoscaling berdasarkan ambang utilisasi CPU dan memori.
- **Keamanan dan Kepatuhan:** Seluruh transmisi data wajib menggunakan TLS 1.3, dengan hasil VAPT awal berstatus Zero Critical dan Zero High Vulnerabilities sebelum produksi.
- **Tata Kelola:** Spesifikasi API harus 100% patuh terhadap OpenAPI 3.0 dan divalidasi melalui automated linter pada pipeline CI/CD.

9. Rekomendasi Teknologi

Implementasi API Management Fase 1 diarahkan untuk menggunakan teknologi yang telah matang, enterprise-ready, memiliki kemampuan high availability dan scalability, serta mendukung integrasi dengan lingkungan infrastruktur dan keamanan yang tersedia di organisasi.

Pemilihan produk atau platform API Management dilakukan dengan mempertimbangkan kesesuaian terhadap kebutuhan fungsional, non-fungsional, keamanan, integrasi, operasional, serta kemampuan pengembangan pada fase selanjutnya. Penyedia dapat menawarkan produk komersial,

open-source enterprise, maupun kombinasi beberapa teknologi sepanjang memenuhi seluruh requirement yang ditetapkan dalam KAK.

Teknologi yang digunakan wajib mendukung standar dan protokol terbuka serta menghindari ketergantungan terhadap teknologi tertentu (*vendor lock-in*) sejauh memungkinkan. Berikut rekomendasi teknologi berdasarkan Area

Area	Technology Baseline / Requirement
API Gateway	Enterprise-grade API Gateway, mendukung REST/HTTP(S), routing, policy enforcement, transformation, rate limiting, circuit breaker
API Management	API lifecycle, API Catalog, subscription, access management, versioning
Developer Portal	Self-service portal, API documentation, application registration, subscription
IAM	OAuth2 / OIDC, JWT, JWKS, client registration, scope & claim
API Standard	**OpenAPI 3.0**
Security	WAF, DDoS protection, IP filtering, rate limiting, threat protection
Transport Security	**TLS 1.3**
Load Balancer	HA, health check, active-active/load balancing
Container/Platform	Mendukung VM/container/Kubernetes sesuai environment yang disepakati
Configuration Management	Git-based version control dan Configuration-as-Code
Observability – Metrics	Prometheus atau teknologi setara
Observability – Dashboard	Grafana atau teknologi setara
Logging	Fluent Bit/Logstash + Elasticsearch/Loki atau teknologi setara
Tracing	Distributed tracing dan correlation/trace ID
CI/CD	Mendukung automated API validation/linting dan deployment pipeline
Security Testing	Vulnerability Assessment & Penetration Testing

10. Tenaga Ahli

Posisi	Jumlah	Kualifikasi Minimum	Peran
Project Manager	1	1. Pendidikan: Minimal Sarjana (Strata 1) dalam bidang Teknologi Informasi, Sistem Informasi, Teknik Informatika, Ilmu Komputer, atau bidang keilmuan lain yang relevan. 2. Pengalaman di bidang Teknologi Informasi: Memiliki pengalaman kerja paling sedikit 7 (tujuh) tahun di bidang Teknologi Informasi. 3. Pengalaman proyek: Memiliki pengalaman paling sedikit 5 (lima) tahun dalam	Planning, coordination, risk, reporting, acceptance

		pelaksanaan atau pengelolaan proyek Teknologi Informasi dan/atau proyek integrasi sistem. 4. Pengalaman API Management: Memiliki pengalaman dalam implementasi, konfigurasi, pengembangan, atau pengelolaan platform API Management.	
Solution/API Management Architect	1	1. Pendidikan: Minimal Sarjana (Strata 1) dalam bidang Teknologi Informasi, Sistem Informasi, Teknik Informatika, Ilmu Komputer, Arsitektur Sistem Informasi, atau bidang keilmuan lain yang relevan. 2. Pengalaman di bidang Teknologi Informasi: Memiliki pengalaman kerja paling sedikit 8 (delapan) tahun di bidang Teknologi Informasi. 3. Pengalaman Arsitektur dan Integrasi Sistem: Memiliki pengalaman paling sedikit 5 (lima) tahun dalam perancangan, pengembangan, implementasi, atau pengelolaan arsitektur sistem dan integrasi sistem Teknologi Informasi. 4. Pengalaman API Management: Memiliki pengalaman paling sedikit 3 (tiga) tahun dalam implementasi, konfigurasi, pengembangan, atau pengelolaan platform API Management.	Architecture, HLD/LLD review, Control/Data Plane, HA, integration
API Gateway/API Management Engineer	1–2	1. Pendidikan: Minimal Sarjana (Strata 1) dalam bidang Teknologi Informasi, Sistem Informasi, Teknik Informatika, Ilmu Komputer, atau bidang keilmuan lain yang relevan. 2. Pengalaman di bidang Teknologi Informasi: Memiliki pengalaman kerja paling sedikit 5 (lima) tahun di bidang Teknologi Informasi. 3. Pengalaman Implementasi API Gateway dan API Management: Memiliki pengalaman paling sedikit 3 (tiga) tahun dalam pelaksanaan implementasi, konfigurasi, pengembangan, atau pengelolaan API Gateway dan/atau platform API Management.	Installation, configuration, routing, policy, HA, troubleshooting
API Security Specialist	1	1. Pendidikan: Minimal S1 Teknik Informatika, Sistem Informasi, Ilmu Komputer, Teknologi Informasi, Keamanan Siber, atau bidang terkait. 2. Pengalaman: Memiliki pengalaman kerja minimal 5 (lima) tahun di bidang keamanan teknologi informasi (IT Security/Cyber Security).	OAuth2/OIDC, JWT, WAF, threat protection, hardening, VAPT

		3. Pengalaman Spesifik: Memiliki pengalaman minimal 3 (tiga) tahun dalam bidang API Security dan/atau Application Security, termasuk penerapan pengamanan API dan aplikasi, identifikasi serta mitigasi kerentanan, authentication dan authorization, serta penerapan security control pada API dan aplikasi.	
DevOps/Infrastructure Engineer	1	1. Pendidikan: Minimal S1 Teknik Informatika, Sistem Informasi, Ilmu Komputer, Teknologi Informasi, atau bidang terkait. 2. Pengalaman: Memiliki pengalaman kerja minimal 5 (lima) tahun di bidang Infrastruktur Teknologi Informasi dan/atau DevOps. 3. Pengalaman Spesifik: Memiliki pengalaman dalam perancangan, implementasi, konfigurasi, dan pengelolaan High Availability (HA), Continuous Integration/Continuous Delivery (CI/CD), serta platform infrastruktur dan aplikasi. 4. Pengalaman Teknis: Memahami dan memiliki pengalaman dalam pengelolaan server, container/platform, deployment automation, monitoring, serta availability dan reliability platform.	Environment, deployment, HA, CI/CD, monitoring
QA/Test Engineer	1 support	1. Pengalaman: Memiliki pengalaman kerja minimal 3 (tiga) tahun dalam bidang Software Testing dan/atau System Integration Testing. 2. Pengalaman Spesifik: Memiliki pengalaman dalam perencanaan, penyusunan test scenario dan test case, pelaksanaan pengujian, pencatatan hasil pengujian, defect tracking, serta pelaporan hasil pengujian sistem dan integrasi. 3. Pengalaman Tambahan: Memiliki pengalaman dalam Performance Testing dan/atau Security Testing menjadi nilai tambah.	SIT, UAT, performance, failover, evidence
Technical Writer	1	1. Pendidikan: Minimal S1 Teknik Informatika, Sistem Informasi, Ilmu Komputer, Teknologi Informasi, Komunikasi, atau bidang terkait. 2. Pengalaman: Memiliki pengalaman kerja minimal 3 (tiga) tahun dalam bidang dokumentasi Teknologi Informasi (IT Documentation). 3. Pengalaman Spesifik: Memiliki pengalaman dalam penyusunan, pengelolaan,	API specs/catalog documentation, HLD/LLD compilation, User/Admin Guide, SOP/Runbook, release notes, project deliverables.

		pemeliharaan, dan pembaruan dokumentasi API, termasuk dokumentasi menggunakan OpenAPI/Swagger, pengelolaan konten Developer Portal, serta penyusunan Standard Operating Procedure (SOP) dan dokumen teknis terkait. 4. Pengalaman Teknis: Memahami struktur dan dokumentasi REST API, endpoint, request/response, authentication, parameter, error handling, serta mampu menyusun dokumentasi teknis yang mudah dipahami oleh developer, technical team, dan pengguna terkait.	

11. Pengujian dan kriteria penerima

11.1. Metode & Ruang Lingkup Pengujian

Area	Kriteria Penerimaan	Evidence
Gateway Core	Routing path/method/header/query tanpa restart.	SIT result
HA	Tetap melayani saat salah satu node unavailable sesuai desain.	Failover test
IAM	JWT, scope, claim dan OAuth2 tervalidasi.	Authentication test
Portal	Catalog, registration, credential dan access request tersedia.	UAT evidence
Security Policy	Rate limit, payload inspection, IP filtering, threat protection berjalan.	Security test
Observability	Metrics, logs, traces, alerting dan audit trail tersedia.	Dashboard/log/trace
Performance	≥1.500 RPS/TPS dan overhead ≤5 ms p95 sesuai scenario.	Performance report
Security	Zero Critical dan Zero High sebelum production.	VAPT + retest
Governance	OpenAPI 3.0 dan automated linting lulus.	Spec + lint report

11.2. Pelaksanaan UAT

1. Internal consumer mengakses API dengan token valid.
2. Mitra eksternal melakukan registrasi aplikasi melalui Developer Portal.
3. Consumer mengajukan subscription/access API.
4. Request tanpa token/expired token ditolak.
5. Scope/claim tidak sesuai ditolak.
6. Request melebihi rate limit ditolak dan tercatat.
7. Payload melebihi batas atau mengandung pola serangan ditolak.
8. Backend failure diuji untuk resilience/failover sesuai desain.
9. Metrics, logs, traces dan alert dapat ditelusuri.
10. Credential rotation dapat dilakukan sesuai lifecycle.

11.3. Acceptance Criteria

Area	Kriteria Penerimaan	Bukti / Evidence
API Gateway Core	Gateway mampu melakukan routing berbasis path, method, header, dan query parameter tanpa restart service.	Hasil SIT routing dan konfigurasi rute.
High Availability	Gateway berjalan dalam mode HA dan tetap melayani trafik saat salah satu node tidak tersedia.	Hasil failover test dan health check report.
IAM & Token Validation	Gateway dapat memvalidasi JWT, scope, claim, dan grant OAuth2 yang disepakati.	Hasil test autentikasi dan token validation.
Developer Portal	Developer dapat melihat katalog API, melakukan registrasi aplikasi, memperoleh kredensial, dan mengajukan akses API.	UAT portal dan screenshot workflow.
Security Policy	Rate limiting, payload inspection, IP filtering, dan threat protection berjalan sesuai baseline policy.	Log pengujian policy dan hasil security validation.
Observability	Metrics, log, trace, alerting, dan audit trail tersedia pada dashboard terpusat.	Dashboard monitoring dan contoh log/trace.
Performance	Platform memenuhi target throughput minimum 1.500 RPS/TPS dan tambahan latensi gateway maksimum 5 ms pada p95 untuk request standar.	Performance test report.
Security Assessment	Hasil VAPT menunjukkan Zero Critical dan Zero High Vulnerabilities sebelum produksi.	Laporan VAPT dan bukti remediation.
Documentation & Governance	Dokumentasi API tersedia dalam standar OpenAPI 3.0 dan lulus automated linting.	OpenAPI specification, linting report, dan approval governance.

12. Risiko dan Mitigasi

Kategori Risiko	Deskripsi Risiko	Dampak	Pemilik Risiko	Strategi Mitigasi Minimum
Integrasi Sistem	Sistem *backend legacy* lambat merespons atau tidak memiliki dokumentasi OpenAPI/Swagger.	Tinggi	Bersama (KBI & Vendor)	Vendor wajib melakukan asesmen awal arsitektur (*discovery phase*) dan menyiapkan mekanisme *mock service/wrapper* atau alternatif integrasi yang sesuai.
Keamanan (Security)	Kebocoran data, konfigurasi tidak aman, atau celah keamanan pada API Gateway/Data Plane.	Kritis	Vendor	Wajib menerapkan *security hardening*, enkripsi, authentication/authorization, secure configuration, serta memenuhi hasil pengujian keamanan sebelum *cut-over production*.
Ketersediaan SDM	Penggantian Tenaga Ahli inti di tengah pelaksanaan pekerjaan.	Sedang	Vendor	Penggantian Tenaga Ahli harus mendapatkan persetujuan KBI terlebih dahulu dengan kualifikasi yang setara atau lebih tinggi.
Downtime/Gangguan Layanan	Gangguan terhadap sistem eksisting selama proses deployment, migrasi, atau perubahan konfigurasi *traffic*.	Tinggi	Bersama (KBI & Vendor)	Deployment dilakukan pada *maintenance window* yang disepakati, disertai *rollback plan* dan prosedur pemulihan yang telah diuji.
Kinerja & Skalabilitas	API Gateway tidak mampu memenuhi kebutuhan *traffic*, *concurrent request*, *latency*, atau pertumbuhan jumlah API.	Tinggi	Vendor	Vendor wajib melakukan *performance testing/load testing* dan memastikan kapasitas platform memenuhi kebutuhan yang ditetapkan dalam KAK serta dapat dikembangkan sesuai kebutuhan.
Kegagalan Implementasi/Migrasi	Migrasi konfigurasi, API, *routing*, policy, atau traffic dari lingkungan eksisting menyebabkan fungsi API tidak berjalan sesuai kebutuhan.	Tinggi	Bersama (KBI & Vendor)	Vendor wajib menyediakan *migration plan*, *test plan*, *rollback plan*, serta melakukan SIT/UAT sebelum implementasi produksi.

Vendor wajib menyampaikan metodologi manajemen risiko sebagai bagian dari proposal teknis, yang sekurang-kurangnya mencakup identifikasi risiko, analisis risiko, rencana mitigasi, monitoring risiko, eskalasi risiko, serta mekanisme penanganan risiko selama pelaksanaan pekerjaan.

Risk Management Plan dapat diperbarui selama pelaksanaan pekerjaan berdasarkan hasil assessment, perubahan kondisi teknis, perubahan ruang lingkup, atau risiko baru yang teridentifikasi.

13. Jangka Waktu Pelaksanaan Pekerjaan

Jangka waktu pelaksanaan pekerjaan adalah selama **3 (tiga) bulan** kalender, terhitung sejak tanggal penandatanganan Surat Perintah Kerja (SPK) sampai dengan seluruh pekerjaan dan deliverable dinyatakan selesai dan diterima oleh Pemberi Kerja.

14. Kewajiban para pihak

Pengaturan yang mengikat secara hukum mengenai hak, kewajiban, dan sanksi bagi Para Pihak akan dituangkan secara lebih rinci dan definitif di dalam **Surat Perintah Kerja (SPK)** atau Perjanjian Kerja Sama. Namun, sebagai acuan teknis dan operasional selama masa pelaksanaan proyek, pihak Penyedia Jasa (Vendor) memiliki kewajiban sekurang-kurangnya sebagai berikut:

14.1. Penyedia

1. **Menyediakan Personel Sesuai Kualifikasi**
   - Penyedia Jasa wajib menyediakan dan menugaskan Tenaga Ahli (seperti *Project Manager, Architect, Engineer, QA*, dan *Technical Writer*) yang profil, pengalaman, dan kompetensinya memenuhi syarat minimum yang tercantum di dalam KAK ini.
   - Selama masa proyek, Penyedia Jasa tidak diperkenankan mengganti Tenaga Ahli inti tanpa pemberitahuan dan persetujuan tertulis dari Pemberi Kerja. Personel pengganti (jika ada) harus memiliki kualifikasi yang setara atau lebih tinggi.
2. **Melaksanakan Pekerjaan Sesuai *Scope* dan *Architecture* yang Disetujui**
   - Seluruh implementasi, konfigurasi, dan instalasi sistem wajib mematuhi Ruang Lingkup Pekerjaan (Scope of Work) yang telah ditetapkan.
   - Eksekusi pekerjaan harus merujuk pada dokumen High-Level Design (HLD) dan Low-Level Design (LLD) serta arsitektur solusi yang telah direviu dan disahkan bersama oleh Para Pihak sebelum fase implementasi (deployment) dimulai.
3. **Menyediakan *Evidence Testing***
   - Penyedia Jasa wajib menyusun skenario pengujian, melaksanakan pengujian, dan menyerahkan bukti pelaksanaan pengujian (testing evidence) yang valid, terukur, dan komprehensif.
   - Bukti pengujian ini mencakup, namun tidak terbatas pada, hasil System Integration Testing (SIT), User Acceptance Testing (UAT), pengujian performa (Stress/Load Test), serta

pengujian keandalan sistem (Failover/HA Test), yang dibuktikan dengan log sistem dan tangkapan layar (screenshot) yang disahkan dalam Berita Acara.

4. **Menjaga Keamanan Informasi Selama Pekerjaan**
   - Penyedia Jasa diwajibkan untuk mematuhi seluruh kebijakan standar keamanan informasi milik Pemberi Kerja, termasuk penandatanganan kesepakatan kerahasiaan (Non-Disclosure Agreement / NDA) atau Klausul yang tersedia pada SPK terkait dengan Keamanan Informasi
   - Tim dari Penyedia Jasa wajib memastikan bahwa seluruh data kredensial (API Key, password, akses server), arsitektur jaringan, dan data sensitif yang diakses selama masa proyek tidak dibocorkan, digandakan, atau disalahgunakan untuk kepentingan di luar lingkup pekerjaan ini.
5. **Melakukan *Remediation* Atas Temuan Dalam *Scope***
   - Penyedia Jasa memikul tanggung jawab penuh untuk melakukan perbaikan teknis (remediation), bug fixing, atau penyesuaian ulang konfigurasi tanpa biaya tambahan apabila terdapat kegagalan fungsional.
   - Kewajiban perbaikan ini berlaku atas setiap temuan ketidaksesuaian (findings) yang muncul pada saat fase SIT, UAT, maupun hasil audit keamanan (Vulnerability Assessment and Penetration Testing / VAPT) yang masih berada di dalam batasan ruang lingkup awal pekerjaan.
6. **Melaksanakan *Knowledge Transfer***
   - Guna menjamin kelangsungan operasional sistem paska-proyek, Penyedia Jasa wajib menyelenggarakan sesi Knowledge Transfer (pelatihan/transfer pengetahuan) kepada tim internal Pemberi Kerja (tim TI, Administrator, atau Developer internal).
   - Proses ini harus dibarengi dengan penyerahan seluruh deliverables kelengkapan dokumen teknis secara final (termasuk User Guide, Admin Guide, Standard Operating Procedure / SOP, Runbook, dan Katalog API).

14.2. Pengguna

1. **Menyediakan Informasi dan Akses Sesuai Kewenangan**
   - Memberikan akses fisik maupun logis yang sah kepada tim Penyedia Jasa (seperti akses ke environment staging/development, infrastruktur jaringan, server, firewall, atau console API Management) sesuai dengan matriks hak akses dan protokol keamanan yang berlaku.
   - Menyediakan dokumen teknis pendukung, spesifikasi antarmuka (interface), kredensial sandbox/testing, serta informasi arsitektur terkait yang dibutuhkan untuk keberhasilan integrasi.
2. **Menetapkan Owner / Stakeholder**
   - Menunjuk dan menetapkan narahubung utama (Single Point of Contact / SPOC), Project Sponsor, Technical Lead, serta Business/Product Owner yang berwenang mengambil keputusan fungsional maupun teknis selama siklus proyek berlangsung.
   - Memastikan ketersediaan stakeholder terkait untuk menghadiri rapat koordinasi rutin (weekly meeting), sesi klarifikasi kebutuhan (discovery workshop), maupun forum eskalasi risiko.

3. **Menyediakan Dependency Internal Sesuai Kesepakatan**
   - Menjamin kesiapan dan ketersediaan sistem backend internal, sistem legacy, atau layanan pihak ketiga yang menjadi ketergantungan (prerequisite) integrasi API Gateway.
   - Menyediakan lisensi pendukung internal, alokasi infrastruktur (VM/kontainer/jaringan), serta mengoordinasikan tim aplikasi internal agar siap pada jadwal pengujian bersama (joint testing) sesuai timeline yang disepakati.
4. **Melakukan Review dan Sign-Off Deliverable**
   - Memeriksa dan memberikan umpan balik (feedback) terhadap draf dokumen yang diserahkan oleh Penyedia Jasa (seperti HLD, LLD, API Spec, SOP, dan Runbook) dalam batas waktu wajar yang disepakati bersama.
   - Menyediakan tim teknis/bisnis untuk memverifikasi serta melaksanakan pengujian penerimaan (SIT/UAT), serta menandatangani Berita Acara Penerimaan / Pengesahan (Sign-off Form) apabila seluruh kriteria penerimaan (acceptance criteria) telah terpenuhi.

15. Serah Terima

Serah terima dilakukan setelah deliverable wajib diterima, acceptance criteria terpenuhi dan selesai atau mengikuti peraturan dan prosedur yang berlaku.

- Berita Acara Serah Terima.
- Daftar deliverable/status acceptance.
- UAT sign-off.
- VAPT/retest evidence.
- As-built document.
- Runbook dan knowledge transfer evidence.

16. Penutup

KAK Ini menjadi acuan pengadaan dan implementasi API Management Platform Fase 1 – Core Foundation. Perubahan scope, requirement, deliverable atau accpetence Criteria melalui mekanisme Change Control dan persetujuan pihak berwenang