

Source BaaS — Core Banking as a Service

Documentação Técnica de Engenharia, Camadas de Segurança, Microserviços (Java/Scala) & Conectividade de APIs

Visão de Engenharia: O Source BaaS foi projetado para operações de alta escala e missão crítica. A arquitetura é desacoplada e modular, utilizando **Java 21 LTS** e **Scala 3 (Akka / Pekko Actors)** no núcleo contábil de partidas dobradas para garantir processamento transacional concorrente atômico e ultra-rápido (sub-120ms), orquestrado por microserviços e gateways em **Node.js / TypeScript / Go** com banco de dados PostgreSQL com **Row Level Security (RLS)**, trilhas imutáveis de auditoria, criptografia AES-256-GCM em repouso e TLS 1.3 em trânsito.

1. Stack Tecnológica de Alta Performance

A infraestrutura combina runtimes compilados de baixa latência e concorrência avançada para atingir 99,99% de SLA e throughput superior a 15.000 TPS:

Camada / Domínio	Tecnologias Utilizadas	Papel no Core Banking
Core Ledger & Transações	Java 21 LTS (Spring Boot 3 / Quarkus), Scala 3 (Pekko/Akka Actor System)	Motor contábil imutável de partidas dobradas, conciliação atômica, isolamento de threads e isolamento financeiro.
Gateway de APIs & Orquestração	TypeScript, Node.js v20+, Go (Golang 1.22+), Envoy / Kong Gateway	Roteamento seguro, rate limiting dinâmico, validação criptográfica HMAC/OAuth2 e proxy reverso mTLS.
Persistência & Ledger DB	PostgreSQL 16+ Enterprise, Supabase (pgvector, RLS), Redis 7 Cluster	Saldos atômicos, particionamento temporal, isolamento rigoroso de tenant via RLS e travas de concorrência.
Event Bus & Filas	Apache Kafka, RabbitMQ, Redis Pub/Sub	Mensageria assíncrona, eventos de auditoria append-only, replay de transações e webhooks com backoff exponencial.
Infraestrutura & Nuvem	Docker, Kubernetes (EKS/GKE), Terraform, Cloudflare Zero Trust	Auto-scaling horizontal, segregação de ambientes Sandbox e Produção, WAF integrado e proteção anti-DDoS.

2. Arquitetura de Blindagem de Segurança (Defense-in-Depth)

A segurança da plataforma opera sob o modelo **Zero-Trust** e cumpre os requisitos mais estritos do Sistema Financeiro Nacional:

- Criptografia Avançada em Repouso e em Trânsito:** Criptografia de envelopes com **AES-GCM de 256 bits** para todos os dados sensíveis armazenados (PII, números de cartão e credenciais bancárias) com chaves gerenciadas via HSM/KMS. Todo o tráfego externo e interno trafega sob **TLS 1.3** com forward secrecy.
- Autenticação Robusta & IAM Blindado (OAuth 2.0 / mTLS / RBAC):** Arquitetura baseada em **OAuth 2.0 com JWT assinado assimetricamente (RS256)**, suporte nativo a **mTLS (Mutual TLS)** para comunicação inter-bancária e parceiros, e **RBAC (Role-Based Access Control) granular** com aprovação dupla em rotinas críticas.
- Sistema Automatizado de Antifraude & Machine Learning:** Motor de regras comportamentais em tempo real com score preditivo, *device fingerprinting* avançado, detecção de velocidade transacional (velocity check), geolocalização anômala, monitoramento de padrões de gastos e *kill-switch* instantâneo para bloqueio de contas suspeitas.
- KYC & KYB Automatizado com Inteligência Biométrica:** Esteira digital com **OCR neural** para extração de dados de CNH/RG/Contratos Sociais, **Prova de Vida (3D Liveness Detection)** com biometria facial, validação cruzada contra bases do governo/Receita Federal e checagem de representação societária.
- Conformidade Estrita com PLD-FT & BACEN:** Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo automatizada: triagem contínua de **Pessoas Expostas Politicamente (PEP)**, listas restritivas internacionais (OFAC, ONU, Interpol, CSNU) e geração nativa de relatórios de comunicação ao **COAF** e **Bacen (SCR 3.040 / Circular 3.978)**.

- **Privacidade e LGPD by Design:** Mapeamento rigoroso de ciclo de vida de dados pessoais, anonimização automática de logs, suporte a direito ao esquecimento e controle estrito de consentimento regulatório.
- **Trilha de Auditoria Imutável (Append-Only Hash Chained):** 100% das requisições, mutações contábeis e acessos administrativos geram registros criptográficos encadeados (SHA-256 hash chaining) impossíveis de serem adulterados ou excluídos retroativamente.

3. Conectores, Adapters e Barramento de Integração de APIs

O Source BaaS possui uma camada agnóstica de **Adapters Intercambiáveis**. A integração com qualquer parceiro bancário ou adquirente é feita via injeção de dependência e parametrização, mantendo o núcleo 100% preservado.

Categoria	Provedores Pré-Mapeados	Mecanismo de Conexão
BaaS & Core Emissores	Dock, Celcoin, Matera, Swap, Pier, Bradesco BACEN SPI	RESTful / ISO 8583 / mTLS com buffers assíncronos e circuit-breakers.
Adquirência & Cartões	Cielo, Rede, Stone, PagBank, Pagar.me, Mastercard MDS	Tokenização PCI-DSS, autorização online sub-100ms e split de liquidação.
KYC & Bureaus de Dados	Unico Check, idwall, Serasa Experian, BigDataCorp, Receita Federal	Webhooks síncronos, matching facial e enriquecimento cadastral em lote.
Webhooks & Event Bus	Event Delivery Engine Interno (para ERPs, Apps e Clientes)	Assinatura HMAC-SHA256, garantia de entrega <i>at-least-once</i> e replay console.

Pipeline de Execução Transacional no Core Ledger:

```
// Pipeline de Execução Transacional Atômica com Auditoria e Antifraude Integrados
public CompletableFuture processPayment(TransferCommand cmd) {
    return riskEngine.screen(cmd) // 1. Antifraude & PEP Screening
        .thenCompose(ok -> ledger.executeDoubleEntry(cmd)) // 2. Partidas Dobradas Atômicas no Core
        .thenCompose(tx -> spiAdapter.dispatchPix(tx)) // 3. Liquidação externa via Adapter SPI/BaaS
        .thenApply(receipt -> auditTrail.logImmutable(receipt)) // 4. Gravação em Trilha Hash-Chained
        .thenApply(receipt -> webhookBus.emit(receipt)); // 5. Notificação assinada com HMAC-SHA256
}
```

4. Conformidade Normativa & Padrões Bancários

A arquitetura cumpre integralmente as resoluções regulatórias aplicáveis a instituições de pagamento e BaaS:

Resolução CMN nº 4.893: Política de Segurança Cibernética, autenticação forte, gestão de incidentes e nuvem segura.	Circular BCB nº 3.978: Procedimentos de Prevenção à Lavagem de Dinheiro (PLD/FT) e comunicação automatizada ao COAF.
Padrão Open Finance Brasil: Arquitetura compatível com especificações FAPI (Financial-grade API) e mTLS.	Isolamento Multi-Tenant & RLS: Proteção lógica com PostgreSQL Row Level Security impedindo acesso cruzado entre contas.

Nota Legal & Propriedade: O código-fonte integral é transferido ao cliente em repositório privado no GitHub com direito de modificação perpétua, personalização completa (White Label) e homologação com a instituição autorizada de escolha.