API Overview

API Overview

Tok provides a REST API for accessing bank account data and initiating payments across Balkan markets.

API Style

Aspect	Detail
Style	REST
Specification	OpenAPI 3.1
Base URL	`https://api.tokapi.io/v1`
Response format	JSON
Auth	API keys (server-to-server) + OAuth2 (PSD2 consent flows)

Authentication

API Key Authentication (Server-to-Server)

All requests require an API key in the `Authorization` header:

```
Authorization: ApiKey tok_live_xxxxxxxxxxxxxxxxxxxx
```

API keys are organisation-scoped. Each Tok client organisation has its own key pair (live + sandbox).

OAuth2 (PSD2 Consent Flows)

When a user connects a bank account, Tok initiates a PSD2 OAuth2 flow:

```
1. POST /v1/consents  →  returns redirect URL to bank's SCA portal
2. User authenticates at bank (SCA: password + SMS/app)
3. Bank redirects to: https://api.tokapi.io/v1/callback?code=XXX&state=YYY
4. Tok exchanges code for access + refresh tokens (stored encrypted)
5. Bank connection active — transactions sync automatically
```

Tokens are stored AES-256-GCM encrypted with GCP Cloud KMS. They are never exposed via API.

Core Endpoints

Accounts

```
GET /v1/accounts
```

Returns all bank accounts connected to the organisation.

```
GET /v1/accounts/{accountId}
```

Returns details for a specific account (balance, IBAN, currency, bank name).

Transactions

```
GET /v1/accounts/{accountId}/transactions
  ?dateFrom=2026-01-01
  &dateTo=2026-03-01
  &limit=100
  &cursor=...
```

Returns paginated transactions for a bank account. Supports cursor-based pagination.

Transaction object:

```
{
  "id": "txn_01HXYZ...",
  "externalId": "BANK-TXN-123456",
  "bookingDate": "2026-02-25",
  "valueDate": "2026-02-25",
```

```
  "amount": "5000.0000",
  "currency": "RSD",
  "direction": "inbound",
  "creditorIban": "RS35105008123123123173",
  "debtorIban": "RS35105008000000019174",
  "remittanceInfo": "Invoice INV-2026-001",
  "source": "open_banking"
}
```

Consents

```
POST /v1/consents
```

Initiate a PSD2 consent flow for a bank. Returns a redirect URL.

```
{
  "bankId": "erste-hr",
  "callbackUrl": "https://app.bilko.io/banking/callback"
}
```

```
GET /v1/consents/{consentId}
```

Returns consent status: `active`, `expired`, `revoked`, or `error`.

```
DELETE /v1/consents/{consentId}
```

Revoke a consent (user disconnects bank).

Payments (PISP — Phase 2, Q3 2026)

```
POST /v1/payments
```

Initiate a payment via bank's payment initiation API (PISP scope).

```
{
  "creditorIban": "RS35105008123123123173",
  "amount": "1500.00",
  "currency": "RSD",
```

```
  "remittanceInfo": "Invoice INV-2026-042"
}
```

Multi-Tenancy

Every API call is scoped to an **organisation**. The organisation is determined by the API key.

- No cross-organisation data access is possible
- Bank connections, consents, and transactions are all organisation-scoped
- Each organisation can have multiple users with different roles

---

Rate Limiting

Rate limits are per-organisation, per-tier.

Tier	Requests / minute	Burst
Free	60	10
Pro	300	50
Enterprise	1,000	200

Rate limit headers on every response:

```
X-RateLimit-Limit: 300
X-RateLimit-Remaining: 287
X-RateLimit-Reset: 1741100460
```

When rate limited, the API returns `429 Too Many Requests` with a `Retry-After` header.

SDKs

Official SDKs handle authentication, retries, and response parsing.

SDK	Language	Package	Install
Node.js SDK	TypeScript	`@tokapi/sdk`	`npm install @tokapi/sdk`
Python SDK	Python 3.10+	`tokapi-sdk`	`pip install tokapi-sdk`

SDK	Language	Package	Install
Kotlin SDK	Kotlin	`io.tokapi:sdk-kotlin`	Gradle: `implementation("io.tokapi:sdk-kotlin:1.0.0")`

Node.js quickstart:

```
import { TokClient } from '@tokapi/sdk';

const tok = new TokClient({ apiKey: 'tok_live_xxxx' });

const accounts = await tok.accounts.list();
const transactions = await tok.transactions.list(accounts[0].id, {
  dateFrom: '2026-01-01',
  dateTo: '2026-03-01',
});
```

Python quickstart:

```
from tokapi import TokClient

tok = TokClient(api_key="tok_live_xxxx")
accounts = tok.accounts.list()
transactions = tok.transactions.list(accounts[0].id, date_from="2026-01-01")
```

Error Format

All errors follow a consistent structure:

```
{
  "error": {
    "code": "CONSENT_EXPIRED",
    "message": "The bank consent has expired. Please reconnect the bank account.",
    "requestId": "req_01HXYZ..."
  }
}
```

Common error codes:

Code	HTTP	Meaning

`INVALID_API_KEY`	401	API key missing or invalid
`CONSENT_EXPIRED`	403	90-day PSD2 consent expired
`CONSENT_REVOKED`	403	User revoked consent at bank
`BANK_API_ERROR`	502	Bank API unavailable
`RATE_LIMITED`	429	Organisation rate limit exceeded
`NOT_FOUND`	404	Resource not found

OpenAPI Spec

The full machine-readable OpenAPI 3.1 specification is at:

- File: `docs/api/openapi.yaml` in the Tok repository
- Developer portal: developer.tokapi.io

Sandbox

All API keys come in pairs: `tok_live_*` and `tok_sandbox_*`. Use sandbox keys for development — sandbox data is not real bank data and does not trigger real bank connections.

Sandbox base URL: `https://sandbox.api.tokapi.io/v1`

Revision #3
Created 2026-03-04 05:07:45 UTC by John
Updated 2026-05-31 20:04:42 UTC by John