# 第一创业证券企业标准

Q/FCSC 001-2024

# API 企业内发布规范

API Published Specifications within the Enterprise

2024-08 发布　　2024-08 实施

第一创业证券股份有限公司

# 目　　次

# 前　言

本文件按照 GB/T1.1-2020 《标准化工作导则 第一部分：标准化文件的结构和起草规则》的规定起草。

本文件由第一创业证券股份有限公司提出。

本文件由第一创业证券股份有限公司归口。

本文件主要起草部门：第一创业证券股份有限公司信息技术中心。

本文件主要起草人：刘耀东、陈志浩、樊金峰、冯元贞、高俊、何力、贺林杰、侯心宇、吉晶、李庶原、瞿任雄、唐钉波、薛海波、靳旭、张俊跃。

# API 企业内发布规范

## 1 范围

本文件规定了第一创业证券股份有限公司的 API 在企业内发布的可观测性、安全性、管理的要求。

本文件适用于用于企业内部系统间集成的 API。

## 2 引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

《证券基金经营机构信息技术管理办法》（中国证券监督管理委员会令 第 179 号 附件一）。

## 3 定义和术语

**API**

应用程序编程接口（英语：Application Programming Interface，简称：API），是一些预先定义的函数，目的是提供应用程序与开发人员基于某软件或硬件得以访问一组例程的能力，而又无需访问源码，或理解内部工作机制的细节。

**SDK**

软件开发工具包（Software Development Kit），也称为开发包或者开发工具包。SDK 通常是由一个或多个软件开发工具组成的集合，用于帮助开发者创建、测试和部署软件应用程序。

**监控系统**

对信息系统的数据采集收集、解析和处理，并实时分析、展示、响应事件。对信息系统提供即时安全警报、及时控制和可靠的系统运行。

## 4 API 技术及安全要求

### 4.1. API 技术基本要求

a) API 建议以 Web 服务或者 SDK 的形式发布。

b) API 被调用后，除了返回数据 Data 参数，还应返回结果码 Code 及结果说明 Msg。

c) API 在发布前，所属系统应纳入统一监控的范围，并在监控系统中可观测 API 的相关信息。

d) API 应用程序接口应具有连接超时限制功能。

e) API 应用程序接口应具备接口主动断开连接的功能，具备发现恶意连接可主动处理的能力。

### 4.2. API 鉴权机制要求

a) API 所属系统为每个调用方系统分配单独的 ID 和口令。

b） API 接口需要求具备身份认证功能，接口身份认证应使用如下要素组合，包括 ID、数字证书、公私钥对。涉及交易接口需考虑双因子认证。

c） API 接口交互安全需对交互数据有效性验证，如接口版本、参数格式是否与平台设计保持一致。涉及交易接口需考虑数字签名来保护交互数据完整性和不可抵赖性。

d） 应根据不同的应用方的服务需求，按照最小授权原则，对其相应 API 接口权限进行授权管理。

### 4.3. API 防护能力要求

a） Web 类 API 接口应对常见网络攻击具有安全防护能力，例如防 SQL 注入攻击、横向越权攻击、拒绝服务攻击等。

b） SDK 应具备静态逆向分析防护能力、动态调试防护能力。

c） 应对 API 接口加密密钥进行安全管理，加密和签名应分配不同的密钥，且相互分离。不应以编码的方式将私钥明文（或密文）编写在 API 应用程序相关代码中。私钥不应存储于 API 与应用方本地配置文件中，防止因代码泄露引发密钥泄露。应根据应用程序接口等级设置不同的密钥有效期，并对密钥进行定期更新。

### 4.4. 用户隐私要求

未经授权，不应通过 API 采集、存储用户个人金融信息或支付敏感信息；如是外部采购 API，在合作终止后，应依据与公司的约定的方式删除（或销毁）通过 API 应用程序接口获取的我司及其用户的相关数据。

## 5 API 管理流程

### 5.1. 发布流程

录入 API 信息、主管审核、架构专家小组审核、API 发布。

### 5.2. 下架流程

提交 API 下架、主管审核、架构专家小组审核、API 变更下架。

### 5.3. 鉴权申请流程

提交 API 消费申请、API 所属系统责任人审核、架构专家小组审核、自动生成鉴权口令。

## 6 API 可观测要求

### 6.1. API 监控

a） 应对 API 接口使用情况进行监控，记录完整访问日志。

b） API 集成关系可观测，由监控系统提供集成关系链路图。

c） 应对 API 所属系统的服务器运行状态、API 服务状态（包括耗时、交易量、成功率等参数）进行监控。

d） 应具备 API 异常监测能力，异常监测内容包括不限于 API 应用程序接口调用并发数、单位时间最大交易调用量等。

### 6.2. API 预警

a） 对于提供给其他系统访问但没有提交发布流程的 API，应可捕获并给技术架构人员预警。

b） 对于乱用鉴权的调用方，应可捕获并给技术架构人员预警。

c） 对于 API 系统资源不足，超过设定阈值时应进行预警。

## 7 API 内部发布管理平台

### 7.1. API 可视化管理功能要求

a） 对于 API 应有 API 发布管理平台，对 API 进行可视化管理。

b） 应对 API 应用接口版本进行管理，建立 API 使用台账，对 API 使用状态进行跟踪。

c） API 的接口参数说明、性能说明、所属系统的访问链接，应在平台中展示。

d） API 的信息中，应包含 API 的被调用及调用其他 API 的集成关系图，并将信息进行存储。

e） 平台宜提供 API 的模拟调用工具，方便调用方验证。

### 7.2. 其他功能要求

a） 应包含系统集成鉴权模块，用于管理系统集成所需鉴权信息。

b） 应包含预警功能，对于没有申请调用鉴权的 API 调用进行捕获并预警。

c） 不应将 API 发布管理平台开放到互联网，其登入应采取 HTTPS 方式。

d） 应具备流量监控、故障隔离、黑名单控制等应用程序接口调用控制能力。

## 8 API 治理组织

为保障 API 的稳健运行及满足服务治理的要求，应设置相应治理团队。

团队包含各领域技术架构人员：负责不满足规范的 API 进行督导整改、API 发布、下架的影响分析及审核；API 内部发布平台管理员：负责平台的权限管理及运维；API 发布方：应业务及其他项目需求，发布及下线 API，并根据规范持续完善 API。