ICS 03.060
CSS A 11

JR

中 华 人 民 共 和 国 金 融 行 业 标 准

XX/T XXXXX—XXXX

证券期货业互联网应用程序接口安全规范

API Security specification for internet application of securities and futures industry

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国证券监督管理委员会　　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由全国金融标准化技术委员会证券分技术委员会（SAC/TC 180/SC4）提出。

本文件由全国金融标准化技术委员会（SAC/TC 180）归口。

本文件起草单位：中国证券监督管理委员会科技监管局、浙商证券股份有限公司、中证信息技术服务有限责任公司、 恒生电子股份有限公司、 安恒信息技术股份有限公司、深圳证券交易所、思迪信息技术股份有限公司、中国信息通信研究院、南方基金管理股份有限公司、永安期货股份有限公司、国泰君安证券股份有限公司、上海金仕达软件有限公司、金证科技股份有限公司、杭州财人汇网络股份有限公司、北京易道博识科技有限公司。

本文件主要起草人：姚前、蒋东兴、周云晖、程立、赵伟江、黄玉锋、陈志勇、周位壬、马进朝、吴美艳、董攀峰、易庆丰、葛峰、谷梦林、陈凯晖、唐海波、秦建津、陈辽勇、胡锦云。

引　言

随着技术的发展，特别是互联网、移动互联网、大数据技术的发展，证券期货业在面向用户服务的技术运用上呈现了好的趋势：一方面，经营机构普遍重视技术研发，服务开始呈现差异化，经营机构服务核心竞争力普遍得到大幅提升；另一方面，为用户提供的服务日趋丰富，用户服务的便捷性、体验和5-10年前比大幅提升，行业整体服务水平得到大幅提高。

但近年来，个人信息泄漏事件频发，各个行业都受到波及，而金融行业所面临的投资者信息更加敏感，在网上业务办理过程中的安全问题尤其严峻。如果经营机构系统存在安全隐患，被不法分子利用，将导致客户个人隐私数据和敏感数据泄露，甚至导致证券期货经营机构数据库客户或用户数据全部泄露的重大安全风险。

分析其根源，近十年证券期货业提供的在线服务发生了以下变化：

a)　服务群体由单纯的投资者扩展至更广泛的用户；

b)　服务内容由行情交易扩展至账户、行情交易、理财、资讯等综合服务；

c)　服务终端由原单一交易工具向多终端产品发展；

d)　研发模式由周边单一开发商变成多开发商、自开发，技术架构日趋复杂。

从证券期货经营机构系统方面，面向互联网服务提供的接口功能不再限于原来登录、交易委托及订单查询，还增加了账单查询分析、账户业务办理、客户资料维护等，甚至还提供账户找回、密码重置、电子合同签约等传统需要临柜交互的功能，接口的业务复杂度、管理复杂度大。

目前，该类互联网接入接口更多关注功能性，对安全管理尚缺乏相应的规范指引，导致部分接口存在鉴权机制不完备、安全控制差等安全隐患。因此，面向互联网接入的服务需要进行治理，采取多种手段和机制的安全管理模式。

证券期货业互联网应用程序接口安全规范

1 范围

本文件规定了证券期货行业互联网应用程序接口的类别与安全属性、安全级别、安全设计、安全运维、安全管理等几方面的安全技术规范与安全保障要求。

本文适用于证券期货行业互联网应用程序的设计与应用，指导提供证券期货应用程序接口服务的金融机构、接口服务应用方规范地、安全地开展接入工作。另外可以为安全评估机构等单位进行安全检查和评估提供一定地参考，其他类型应用程序接口安全设计和应用也可以参考本文规范。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术术语

JR/T 0060-2010 证券期货业信息系统安全等级保护基本要求

JR/T 0192-2020 证券期货业移动互联网应用程序安全规范

JR/T 0158-2018 证券期货业数据分类分级指引

JR/T 0185-2020 商业银行应用程序接口安全管理规范

3 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T25069-2010某些术语和定义。

3.1

应用程序接口 application programming interface

根据需求预先定义的功能，使用者可以通过该功能或组合功能访问服务器并获取结果，无需关注服务端的设计与实现。

3.2

应用软件开发工具包 software development kit

基于某特定软件包、软件框架、硬件平台、操作系统等建立应用程序时所使用的软件开发工具集合。

3.3

应用唯一标识 application unique ID

申请方应用被验证通过后，根据一定规则，由服务方颁发的唯一标识。

3.4

应用密钥 application secret

应用调用接口校验凭证，与应用唯一标识配套使用，以验证通过接口接入应用的合法性，验证通过即可调用服务提供的功能。

3.5

安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。

[来源：GB/T 25069-2010，2.2.1.6]

3.6

敏感信息 sensitive information

由权威机构确定的必须受保护的信息，该信息的泄露、修改、破坏或丢失对人或事产生可预知的损害。

[来源：GB/T 25069-2010，2.2.4.7]

3.7

授权 authorization

赋予某一主体可实施某些动作的权利的过程。

[来源：GB/T 25069-2010，2.1.33]

4 缩略语

下列缩略语适用于本文。

API	应用程序接口
SDK	应用软件开发工具包
HTTP	超文本传输协议
App_ID	应用唯一标识
App_Secret	应用密钥
SSL	安全套接层协议
TLS	安全传输层协议
MAC	消息鉴别码

5 证券期货行业系统及接口概述

5.1 整体架构

证券期货应用程序接口服务是一种依托 API 技术实现内部与外部互联的金融服务模式。证券期货机构通过提供互联的应用程序接口服务，输出自身金融服务能力与信息技术能力。

外部各种客户端应用能够通过互联网渠道，调用证券期货应用程序服务接口，获取证券期货机构提供的各类服务，其逻辑架构见图：

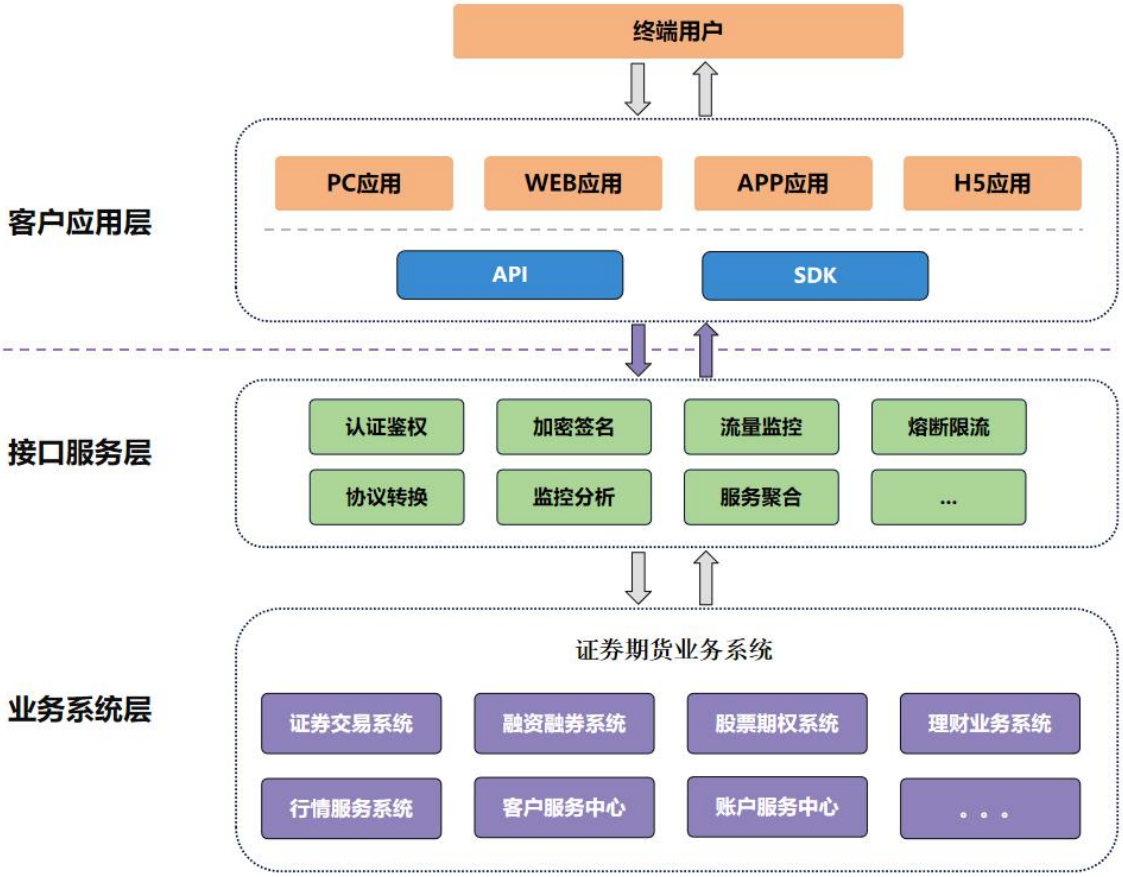

图 1 整体架构

证券期货应用程序接口服务的参与方主要包括终端用户、客户应用方，证券期货机构方通过 API 直接连接或 SDK 间接连接方式向客户应用方和终端用户提供应用程序接口服务，实现证券期货机构服务的对外输出。

终端用户通过客户应用方发起证券期货应用程序接口应用请求，并接收由客户应用方返回的处理结果。

客户应用方负责接收并处理终端用户的请求操作，通过应用程序接口向证券期货机构方提交相关请求、接收返回结果，依照流程进行服务请求处理或反馈终端用户。

证券期货机构方构建证券期货应用程序接口、应用程序接口服务层和证券期货业务系统以提供证券期货应用程序接口服务。证券期货应用程序接口服务层将应用方请求转发至证券期货业务系统处理，并将处理结果反馈应用方及终端用户，包含认证鉴权、加密签名、流量控制、熔断限流、协议转换、监控分析、服务聚合等功能，不涉及具体业务逻辑处理，实现对证券期货应用程序接口和客户应用方的管理，通讯安全和数据传输安全主要在本层实现。

业务应用层主要是证券期货行业对外提供服务的业务系统，包含证券交易系统、融资融券系统、股票期权系统、理财业务系统、行情服务系统、客户服务中心、账户服务中心以及其他业务系统。

5.2 接口类别说明

API 是前端调用后端数据的通道的，API 的调用方可以通过开放的 API 访问证券期货提供的各类服务接口，完成操作与数据交互。API 调用方即 API 的服务对象，为调用 API 的用户（应用程序），服务对象基本可以分为合作机构、外部用户、内部用户、内部应用四种类型。本文件只讨论通过互联网访问的服务对象即合作机构，外部用户与内部用户。其中合作机构一般通过后端应用服务来调用 API。

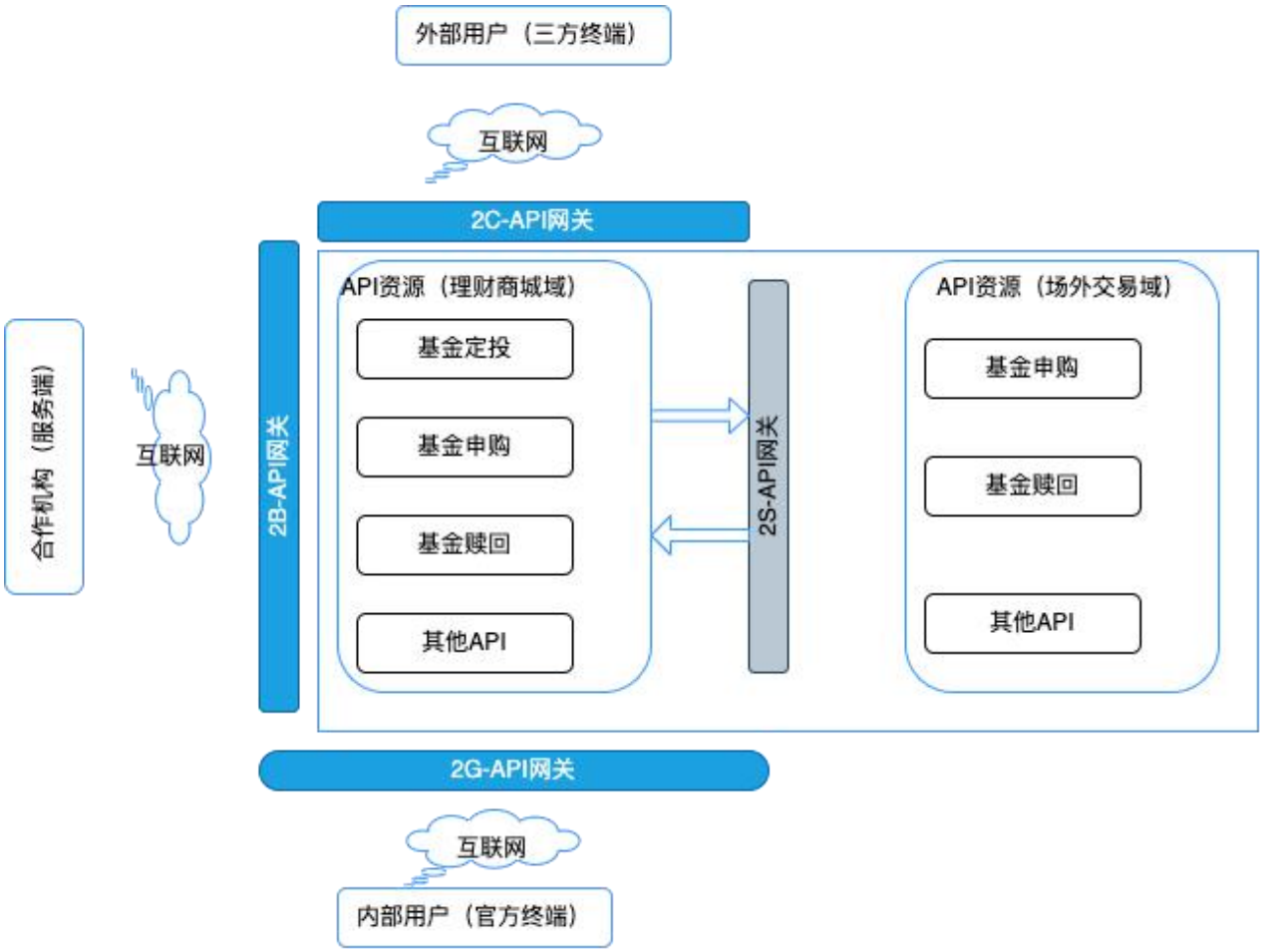

图 2 接入说明

根据调用方的不同纬度，将对外的 API 分为：

a) toB 类接口的服务对象主要为合作机构，并在其特定的服务端完成对特定接口的调用；
b) toC 类接口的服务对象主要是外部用户，外部用户通过外部机构的客户端，完成对特定接口的调用；
c) toG 类接口的服务对象主要是内部用户，内部用户通过内部的终端完成特定接口的调用。

6 接口安全分级

6.1 安全属性

a) 保密性定义：也称机密性，是不将有用信息泄漏给非授权用户的特性。可以通过信息加密、身份认证、访问控制、安全通信协议等技术实现，信息加密是防止信息非法泄露的最基本手段，主要强调有用信息只被授权对象使用的特征；
b) 完整性定义：是指信息在传输、交换、存储和处理过程中，保持信息不被破坏或修改、不丢失和信息未经授权不能改变的特性，也是最基本的安全特征；
c) 可用性定义：也称有效性，指信息资源可被授权实体按要求访问、正常使用或在非正常情况下能恢复使用的特性（系统面向用户服务的安全特性）。在系统运行时正确存取所需信息，当系统遭受意外攻击或破坏时，可以迅速恢复并能投入使用。是衡量网络信息系统面向用户的一种安全性能，以保障为用户提供服务；

d) 可控性定义：指网络系统和信息在传输范围和存放空间内的可控程度。是对网络系统和信息传输的控制能力特性；
e) 不可否认性定义：又称拒绝否认性、抗抵赖性，指网络通信双方在信息交互过程中，确信参与者本身和所提供的信息真实同一性，即所有参与者不可否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

6.2 安全级别

根据接口对接的数据级别的影响程度（严重、中等、轻微、无），一般指数据安全属性（完整性、保密性、可用性等）遭到破坏后带来的影响大小。证券期货的业务接口安全级别划分为 4 级，安全保护要求从 S0 至 S3 逐级提高，安全级别如下：

a) S0：公开访问接口，具备可控性。接口对应数据的安全属性遭到破坏或损失后，影响范围小，影响程度一般是“轻微”或“无”。一般特征：数据可被公开或可被公众获知、使用；
b) S1：一般访问接口，具备可控性，完整性，可用性。接口对应数据的安全属性遭到破坏或损失后，影响范围可控制在一定范围，影响程度一般是“中等”。一般特征：数据用于一般业务使用，一般针对受限对象公开；
c) S2：私密访问接口，具备可控性，完整性，可用性，保密性。数据的安全属性遭到破坏或损失后，影响范围较大，影响程度一般是“严重”。一般特征：数据用于重要业务使用，一般针对特定人员公开， 且仅为必须知悉的对象访问或使用；
d) S3：核心访问接口，具备备可控性，完整性，可用性，保密性，不可否认性。数据的安全属性遭到破坏或损失后，影响范围大，影响程度一般是“严重”。一般特征：数据主要用于行业内大型或特大型机构中的重要业务使用，一般针对特定人员公开，且仅为必须知悉的对象访问或使用。

证券期货业应用程序接口随着业务的发展，其类别和数量具有较大规模，本文件对其中部分接口进行示例性划分，可参考附录 A。

6.3 动态调整

接口分级并不是定义之后再无进行修改变更，业务创新、系统变化等情况必然需要对级别进行更改，证券期货公司应具备以下几个条件：

a) 证券期货公司对 API 以及所对应数据与资源应建立跟踪机制，包括结合扫描工具、自查上报、访问日志等形成一份完整的 API 清单。清单包括 API 服务对象、作用类型、读写类型、用户鉴权、是否包含个人信息等信息方便确认级别；
b) 通过接口访问日志、调用监控等情况，观察接口涉及的数据内容、服务对象是否发生变化；
c) 接口的变更处理需要进行评审；
d) 系统架构涉及合理，可以应对 API 级别调整后，相应的安全管控能得到调整。

另外，接口提供方应及时跟进重新定义级别，并进行调整管控接口级别升级或降级。

7 接口安全设计

7.1 接口安全控制

7.1.1 接口会话安全控制

证券期货应用系统接口应具备基于会话的安全控制机制。会话管理分为三个阶段：会话建立、会话保持、会话退出。具体要求包括：

a) 会话建立：应用系统应提供会话建立接口，进行会话建立时，接入方需要将接入方编码、IP地址、MAC地址等身份认证信息通过接口送入，应用系统返回会话ID。后续调用方所有请求应送入该会话ID；
b) 会话保持：应用系统需具备会话有效期机制，当接入方无业务操作的时间超过有效期后，应用系统应结束当前会话；
c) 会话退出：接入方退出登录时，需向应用系统发送会话结束请求，使当前会话状态失效，失效后将不允许进行任何接口访问；应用系统可以主动强制会话失效，失效后，接入方不允许使用该会话进行任何接口访问。

7.1.2 接口黑白名单控制

证券期货应用系统接口应具备黑白名单控制机制。系统根据相关验证内容对接入方的身份进行识别，对于黑名单的请求予以拒绝；对于白名单的请求予以通过。具体要求包括：

a) 黑白名单的控制维度至少应包括：接口调用功放、接口、用户等维度；
b) 接口黑白名单应能实时调整和实时生效。设定时应记录接口黑白名单调整日志。

7.1.3 接口权限控制

证券期货应用系统接口应具备接口权限控制机制，对于不具备接口调用权限的接入方请求应予以拦截。具体要求包括：

a) 控制维度：技术维度上，需按照接口接入方、接口及接口字段等维度进行调用权限控制；业务维度上，需要按照业务功能、用户等维度进行调用权限控制；
b) 权限控制功能需要根据接口安全级别来控制，具体包括：
   1) S0级接口：满足接入方要求的均可调用；
   2) S1级及以上接口：需按控制维度进行接口调用权限控制。
c) 接口权限控制需能够根据系统运行情况和业务处理情况进行最小化授权，并能实时调整和实时生效。授权时应记录接口权限调整日志。针对S3级接口，需具有完备的权限管理评估和确认机制；
d) 对于越权访问的接入方应记录阻拦日志，对于频繁越权访问的或有重大安全隐患的，视情节列入应用系统接口黑名单或从白名单中删除。

7.1.4 接口流量控制

证券期货应用系统接口应具备接口流量控制机制。即按照一定时间间隔，对接口调用频次进行实时控制。对于超过规则的访问应予以限制甚至禁止，从而保护应用系统。具体要求包括：

a) 接口流量控制可选择不同的时间间隔，如每秒、每分钟、每小时、每日等；
b) 控制维度：技术维度上，需按照接入方、接口进行流量控制；业务维度上，需要按照业务功能、用户维度进行流量控制。

对于超过流量控制访问的接入方应记录处置日志，对于频繁超速访问的或有重大安全隐患的，视情节列入应用系统接口黑名单。

7.2 接口身份认证安全

接入方通过线上或线下方式提供自己的身份材料、准入资料和条件，同时要通过验证资料的有效性和完整性，并说明业务场景以及需要的相关服务接口。不同安全级别接口需要不同的身份认证方式：

a) 针对S0级接入，至少需要App_ID来标识应用接入方身份；

b) 针对 S1 级接入，基于对于应用方身份认证应使用的验证要素包括：App_ID 与 App_Secret、数字证书、公私钥对其中一个的组合；
c) 对于 S2 及以上级别接口，应用方身份认证时，应使用包含公私钥或数字证书对的方式进行双向身份认证；
d) 用户身份认证应在证券业务系统对于 S2 级别及以上的接口中所涉及的应用服务，用户登录身份认证应至少使用双因子认证（定义）的方式来保护用户应用安全。

7.3 数据安全

7.3.1 网络通信安全

由于目前的系统都是进行多节点分布式网络通讯和数据传输，各节点间会提供服务端口以及数据通讯协议，所以网络层的安全设计，主要集中体现在通讯端口和协议，以及数据传输的安全上。

a) 通讯端口安全设计规范：尽量减少监听端口，内部通讯使用高位端口（1024 以上），外部访问使用通用端口（例如 80、443）；
b) 通讯协议安全设计规范：使用安全通讯握手机制保证合法连接访问控制，使用协商超时保护机制防止恶意并发连接；
c) 数据传输安全设计规范：数据传输使用加密安全通道，避免明文可监听窃取。应采用 SSL/TLS 安全通道通信，建议使用 TLS1.2 以上版本，同时确认通信加密算法是强加密算法，密码长度足够安全。个别系统要求使用国家标准国密进行通信；
d) 移动互联网应用程序与服务器之间重要数据的通信应使用安全的通信协议和加密算法：
   1）S0 级接口：主要是一些公共服务类接口，不涉及重要数据的传输，网络通信安全要求；
   2）S1 及以上接口： 应用程序与服务器之间重要数据的通信应使用安全的通信协议和加密算法。

7.3.2 数据的机密性

移动互联网应用程序与服务器之间重要数据传输时，应采用密码技术保证重要数据传输的机密性。

a) S0、S1 级接口： 不涉及重要数据传输的机密性要求；
b) S2 及以上接口： 应用程序与服务器之间重要数据传输时应采用密码技术保证重要数据传输的机密性。

7.3.3 数据的完整性

移动互联网应用程序与服务器之间重要数据传输时，应采用密码技术保证重要数据传输的完整性。

a) S0 级接口：主要是一些公共服务类接口，无重要数据传输的完整性要求；
b) S1 及以上接口： 应用程序与服务器之间重要数据传输时应采用密码技术（如：数字签名、MAC 等）保证重要数据传输的完整性。

7.3.4 数据的不可否认性

移动互联网应用程序与服务器之间重要数据传输时，应采用密码技术保证重要数据传输的不可否认性。

a) S3 级以下接口：无重要数据传输的不可否认性要求；

b) S3 级接口： 应用程序与服务器之间重要数据传输时应采用密码技术保证重要数据传输的不可否认性，在有条件的情况下应采用数字证书技术。

7.4 接口攻击防护

应用程序接口提供服务需保证 SDK 或其他调用方式的安全防护，具体可体现以下几点：

a) S2 以上级别的接口对应的移动终端应用 SDK 应具备静态逆向分析防护能力，防范攻击者通过静态反汇编、字符串分析、导入导出函数识别、配置文件分析等手段获得有关 SDK 实现方式的技术细节；
b) S2 以上级别的接口对应的移动终端应用 SDK 宜具备动态调试防护能力，包括但不限于：具有防范攻击者通过挂接动态调试器、动态跟踪程序的方式控制程序行为的能力、具有防范攻击者通过篡改文件、动态修改内存代码等方式控制程序行为的能力；
c) 证券接口对应应用系统的安全等级应符合证券期货业网络安全等级保护基本要求，进行安全设计、安全建设、安全保护；
d) 证券接口需具备数据包防重放能力，通过保证请求仅一次有效，需在请求体中携带当前请求的唯一标识等方式防止报文重复发送，避免导致业务发生安全问题。

8 接口运维监控

8.1 运维管理

证券期货公司在提供接口服务时，需要对接口进行严格地、安全地运维管理，根据本文第 7 章安全技术要求需具备包括但不限于以下管理能力：

a) 接口管理：所有对外提供接口都应由接口管控平台进行维护，接口需要进行相应的开发和审批流程以后进行调整为上线状态对外提供服务。若接口经过业务和技术人员确认为退役状态，即可根据相关制度审批后调整为下线状态停止对外提供服务。也以可通过上下线管理进行系统的熔断降级。接口服务终止后相关数据归档、数据删除（或销毁）、信息保护、用户资金和账户安全等问题充分达成一致，明确相关责任，并充分履行用户告知义务，应将有关数据进行归档处理；
b) 密钥管理：主要针对相关的唯一标识 App_ID、App_Secret、数字证书（或公私钥对）等一些与身份认证或安全加密等相关信息进行管理，包括生成、颁发、吊销等操作；
c) 接口权限管理：提供授权和权限管理功能，设定接口使用权限，严格控制业务、用户数据的访问权限和有效期，应按应用方、应用唯一标识 App_ID、接口、用户等维度，依据最小授权原则进行授权。对未授权的调用者禁止访问。可以选择性地对 API 的调用有效期进行控制（比如单次有效、协议期内有效、固定次数有效、固定时间段有效等）。接入请求方可以通过合规流程对接口申请，审核人员通过权限管理授予。应为用户提供关闭应用程序接口相关服务的申请渠道。当管理人员需要解除某调用方的授权接口时，可以查看该调用方授权列表并删除；
d) 接口流量管理：一般接口提供方会对接口调用进行流量控制，根据多维度特征值（比如调用者、微服务域、IP 等），不同时间单位（秒，分钟，小时等）进行设置流量控制，设置包括一些个性化定制流控方案；
e) 黑白名单管理：支持调用方白名单/黑名单管理，可以通过管理平台配置某个接口或某个接口组的白名单/黑名单来允许/拒绝某个来源的请求。比如白名单，支持配置 IP 或者 App_ID + IP 的白名单访问，不在白名单列表的请求将会被拒绝。可控制不同的调用方可根据业务场景选择白名单方式或者黑名单方式；
f) 会话管理：系统有会话运维管理机制，进行会话相关方面的功能操作，比如为保护服务端系统正常运行，可以强制失效某会话，不再允许进行任何接口访问。

8.2 监控与报警

通过监控平台提供可视化接口实时监控，包括：调用量、调用方式、响应时间、错误率，并支持历史情况查询，以便统筹分析。管理人员可以自定义各种报警规则，系统将自行监控并推送告警信息。证券期货公司监控能力需具备包括但不限于以下几点：

a) API 维度统计：指定条件 API 维度统计列表展示，包括：API 平均响应时间、调用次数、正确率、流量等多种纬度报表；统计 API 被消费的情况；从客户端应用的纬度统计其调用 API 总数，调用情况等；
b) 流量监控：根据多维度特征值（比如应用、微服务域、IP 等等），不同时间段（秒，分钟，小时等）进行流量控制，一旦触发流量控制规则时，予以告警、停用，限制接入方，保护后端服务；
c) 异常访问风险监测及预警：制定风险策略，对大规模数据拉取、非工作时间访问、非常用 IP 访问等异常访问就行监测和预警；
d) 支持未授权和冒用的监测，支持故障监测和恢复能力，支持接入方黑名单管理，对黑名单具备识别预警功能；
e) 故障隔离：支持分路隔离：通过负载路由进行分路隔离；应用隔离：将第三方接入应用进行隔离；服务隔离：在 API 维度针对某一个服务进行隔离；系统隔离：在服务系统维度针对某一个服务提供系统进行隔离；
f) 重复发送：可通过监控手段对于一些反复尝试、破坏性攻击等行为进行尝试可以进行一些必要手段进行限制接入；
g) SDK 版本监控：可通过监控手段收集 SDK 信息，对于问题版本可提醒升级等操作；
h) 通道健康检查：可进行系统接入通过健康性检查，包括可用性、通道质量等；
i) 日志分析异常指标：通过日志进行关键信息分析，对于问题可进行告警提醒。

8.3 日志

证券期货公司对应用程序接口运维和监控时需将接口调用情况、接口执行、级别调整、审计以及其他操作过程中关键日志包括但不限于以下几点进行保留：

a) 全链路日志：建设日志中心系统，提供接口调用的全链路分析功能。请求与应答经过网关节点、服务节点时向日志中心发送日志，记录相应的信息。记录包括请求内容、请求的 IP、后端服务的 IP、应答返回内容、请求的响应状态等等诸多的关心的内容，供分析系统在处理时使用；
b) 业务日志：日志中心系统同时具备收集接口提供服务的业务报错日志，甚至可以包括处理关键信息日志。业务分析人员可以通过日志中心搜索功能快速定位接口调用错误详情，分析调用逻辑；
c) 系统异常日志：接口不稳定性可能会给系统带来一些问题或异常，该类日志也应归集到日志中心集中处理，运维人员进行集中分析处理，及时上报处理避免大量调用导致更大问题；
d) 审计留痕日志：一方面支持用户操作日志的记录，记录用户登录、退出以及操作功能点的操作日志，用于留痕备查。另一方面，记录接口访问日志用于查询\审计，包括交易流水号、访问应用、访问接口、访问 IP、调用耗时、时间戳、返回结果等，并对日志记录进行完整性保护，确保日志不被篡改、删除、覆盖。对于日志中涉及账号、支付等敏感信息可进行特殊处理，部分屏蔽；
e) 运维日志：运维操作留痕，如接口上下线，接口到一定时间不再使用之后需要申请下线，并进行备案，接口下线需要完整的流程，应进行标准化、有序的下线机制，对接口下线之后的日志、认证等信息进行规范的留存处理。

附 录 A
（资料性）
接口等级划分示例

A.1 参考

接口等级划分参考见表A.1。

表 A.1 接口等级参考表

行业	安全级别	级别说明	接口类别	模块
证券	S0 级	公开访问接口	行情类	股票、场外基金、资产管理产品、银行理财产品行情接口；区域性股权交易中心、金融资产交易中心行情接口
			资讯类	公开资讯数据接口
	S1 级	一般访问接口	资讯类	授权访问资讯接口
	S2 级	私密访问接口	账户类	证券账户：客户证券账户、客户资金账户、客户信用账户、自营账户及其他证券相关账户的账户开立、变更、销户、证券管理、资金管理、合同管理、适当性管理、业务权限管理、费用管理、交收等接口 理财账户：理财账户开立、变更、销户、持仓管理、资金管理、合同管理、适当性管理、业务权限管理、费用管理、交收等接口 OTC 账户： OTC 账户开立、变更、销户、持仓管理、资金管理、合同管理、适当性管理、业务权限管理、费用管理、交收等接口 自营账户：自营类账户开立、变更、销户、持仓管理、资金管理、适当性管理、业务权限管理、费用管理、交收等接口
	S3 级	核心访问接口	交易类	证券普通交易、融资融券交易、股票质押式回购交易、约定式购回交易、基金交易、期权交易等业务交易委托接口。规范资产管理投资普通交易、融资融券交易、股票质押式回购交易、约定式购回交易、基金交易、期权交易等业务交易委托接口 OTC 市场产品的交易委托接口 场外基金、资产管理产品、银行理财产品交易委托接口
期货	S0 级	公开访问接口	行情类	商品期货、股指期货、原油期货等期货产品行情接口
			资讯类	公开资讯数据接口
	S1 级	一般访问接口	资讯类	授权访问资讯接口
	S2 级	私密访问接口	账户类	期货业客户账户开立、变更、销户、持仓管理、资金管理、合同管理、适当性管理、业务权限管理、费用管理、交收等接口
	S3 级	核心访问接口	交易类	商品期货、股指期货等期货产品交易委托接口
基金	S0 级	公开访问接口	行情类	基金行情信息接口

			资讯类	公开资讯数据接口
	S1 级	一般访问接口	资讯类	授权访问资讯接口、账户登录鉴权验证接口
	S2 级	私密访问接口	账户类	账户开立、批量开户、账户销户、账户资料修改、银行资料修改、密码重置、增开交易账户、换卡、客户资料查询、适当性管理、风险问卷查询接口、风险问卷测评接口等接口
	S3 级	核心访问接口	交易类	基金认购、申购、赎回、预约申购、预约赎回、赎回转购、批量开户、批量交易、基金转换、修改分红方式、撤单、可撤单列表查询、交易申请查询、客户持仓份额查询、分红查询、定期定额协议签订/修改、定期不定额协议签订/修改、资金存入、交易限制维护、基金转托管、联机对账、定投扣款、投顾策略管理、投顾基准管理、投顾大类管理、投顾调仓配置管理、投顾策略业绩分析、投顾组合净值管理、投资组合监控、投顾指令管理、投顾行情管理等接口

参 考 文 献

[1] GB/T 22239—2008 信息安全技术信息系统安全等级保护基本要求
[2] GB/T 25069—2010 信息安全技术术语
[3] JR/T 0192—2020 证券期货业移动互联网应用程序安全规范
[4] JR/T 0060—2010 证券期货业信息系统安全等级保护基本要求
[5] JR/T 0158—2018 证券期货业数据分类分级指引
[6] JR/T 0185—2020 商业银行应用程序接口安全管理规范
[7] 证券公司网上证券信息系统技术指引
[8] 期货公司网上期货信息系统技术指引
[9] 网上基金销售信息系统技术指引