

广东保伦电子股份有限公司

产品接口说明书

产品名称: _____

产品型号: _____

撰写人: _____

所属部门: _____

审 核: _____

目录

一、 概述.....	4
1.1 编写目的.....	4
1.2 适用范围.....	4
1.3 术语说明.....	4
二、 通用规范.....	4
2.1 基础 URL 与接口风格.....	4
2.2 认证.....	5
2.3 请求约定.....	6
2.4 统一响应格式.....	7
2.5 分页.....	8
2.6 通用业务状态码.....	9
2.7 信封例外：文件导出.....	10
2.8 数据字典.....	10
2.9 链路追踪.....	11

一、概述

1.1 编写目的

本文档面向前端开发，定义业务中台后端所有接口共同遵守的全局规范与开发契约，包括认证方式、请求与响应格式、分页结构、错误码体系等跨接口恒成立的规则。

具体业务接口的入参/出参字段，以后续接口文档为准；本文档描述的规则对**所有接口**恒成立。

1.2 适用范围

本文档适用于所有参与业务中台前端设计、开发、测试的团队及个人。

1.3 术语说明

JWT Token：登录后签发的身份令牌，后续所有请求以请求头 `Authorization: Bearer {token}` 携带。

数据字典：由后台统一维护的 `label/value` 键值对，用于下拉框等可配置选项的数据源。

Trace Id：单次请求的全链路日志标识，通过响应头 `X-Trace-Id` 返回，用于问题排查。

二、通用规范

2.1 基础 URL 与接口风格

项	约定
Base URL	按环境提供： <code>http://{host}:{port}</code> （开发/测试/生产地址由后端另行下发）
字符集	UTF-8
URL 形态	<code>/api/{模块}/{资源或动作}</code> ，如 <code>/api/auth/login/dingtalk</code> 、 <code>/api/customer/customers/page</code>
接口风格	非严格 RESTful：单条详情用 GET ，其余（含分页查询、保存、删除）一律 POST + 动作后缀（ <code>/page</code> 、 <code>/saveOrUpdate</code> 、 <code>/delete</code> 等）

为什么不用严格 RESTful（PUT / DELETE / 语义化 URL）：

1. 解决 GET 传输复杂查询的天然缺陷

管理系统的查询条件通常复杂：多选过滤、日期范围、嵌套条件、批量 ID 数组.....这些塞在 GET query 里受 URL 长度限制，难以表达结构化参数。

2. 权限控制、日志审计与限流便利性

系统绕不开按钮级/接口级的权限控制和操作日志审计。/save、/delete 这种 URL 自身就说明操作，「一个操作一个 URL」意味着权限点位、审计规则、网关限流都只需匹配 URL 字符串。

2.2 认证

(1) **登录**：通过钉钉扫码登录换取 token：

```
POST /api/auth/login/dingtalk
```

```
Content-Type: application/x-www-form-urlencoded
```

```
authCode=xxxxxx
```

成功后 data 中返回：

```
{
  "code": 0,
  "success": true,
  "message": "success",
  "data": {
    "token": "eyJhbGciOiJIUzI1NiJ9.xxx.yyy",
    "userInfo": { "userId": "1946xxxxxxxxxxxx", "nickname": "张三" }
  }
}
```

(2) **携带 token**：除登录接口外，**所有请求**都必须携带请求头：

```
Authorization: Bearer {token}
```

(3) **token 生命周期**：

- token 由后端**滑动续期**：只要持续在用，剩余有效期不足一半时后端自动续满。
- token 字符串自签发起固定不变（字符串内不含过期时间，有效期由服务端管理），续期发生在服务端内部，前端无感知、无需替换本地 token。
- 前端**不需要**定时刷新 token，也没有 refresh token 机制。
- 收到 **HTTP 401**（响应体 code=40103）即代表未登录或登录已过期，**此时才**清除本地 token 并跳转登录页。

(4) **登出**：POST /api/auth/logout（携带 token）。登出后该 token 立即失效（即使 JWT 本身未过期）。

(5) **当前用户**：GET /api/auth/me（携带 token）。

2.3 请求约定

(1) 读操作（查询单条 / 列表 / 详情）

- 方法：GET
- 参数：全部放 URL query，如 GET /api/auth/dict/items?dictCode=customer_source

(2) 写操作（保存 / 删除 / 登录等）与分页查询

- 方法：POST
- Content-Type: **默认 application/x-www-form-urlencoded**；仅文件上传接口使用 multipart/form-data。
- 参数：全部为表单字段，不使用 JSON body。

POST /api/auth/system/menus/save

Content-Type: application/x-www-form-urlencoded

Authorization: Bearer {token}

parentId=0&menuName=客户管理&menuType=2&path=/customer&sort=1&visible=true

(3) 复杂字段：JSON 字符串嵌表单

当某个入参是**对象或数组**时，前端将其 JSON.stringify 后作为一个**普通表单字段**传递（是「各复杂字段各自 stringify」，不是整个 body 打包成一个 JSON）：

POST /api/customer/customers/save

Content-Type: application/x-www-form-urlencoded

Authorization: Bearer {token}

name=测试客户&ownerId=1946xxx&contacts=[{"name":"李四","phone":"13800000000"}, {"name":"王五", "phone":"13900000000"}]

上例中 `contacts` 字段的值是 JSON 数组字符串（实际发送时需 URL 编码）。哪些字段是 JSON 字符串字段、其内部结构长什么样，以接口文档中该接口的参数说明为准。

（4）数据类型约定

类型	约定
ID（含所有雪花 ID）	一律按字符串收发。后端返回时已序列化为字符串（超出 JS Number 安全范围，转 Number 会丢精度），前端回传原样传字符串即可
日期时间	yyyy-MM-dd HH:mm:ss，时区 GMT+8
日期	yyyy-MM-dd
时间	HH:mm:ss
布尔	true / false

2.4 统一响应格式

所有接口（文件导出除外，见 2.7）返回统一 JSON 结构：

```
{
  "code": 0,
  "success": true,
  "message": "success",
  "data": { }
}
```

字段	类型	说明
code	number	结果码，0 为成功，其余见 2.6 通用业务状态码
success	boolean	是否成功
message	string	提示信息。失败时为面向用户的中文提示，前端可直接 toast 展示，无需自行映射文案
data	any	业务数据，可能为 null（如保存/删除类接口成功时，对于列表查询，空列表返回 [] 而不是 null），前端须判空

判定规则：

- 判成功：只看 `success === true`。
- 判失败后的分支处理（跳登录、回填表单等）：再看 `code`。

HTTP 状态码：业务失败（参数错误、业务规则不满足等）HTTP 状态码**仍是 200**，只能通过响应体的 `success/code` 判断。仅以下场景 HTTP 状态码非 200：

HTTP	场景	响应体 code
401	未登录 / 登录过期	40103
403	已登录但无权限	40301
404	接口路径不存在	40401
500	系统内部异常	50001

即使 HTTP 状态码非 200，响应体**仍然是统一信封结构**，前端全局拦截器可统一解析。

2.5 分页

（1）入参（POST 表单字段，所有分页接口通用），各业务分页接口在此基础上追加自己的过滤字段：

字段	类型	默认	说明
current	number	1	当前页码，从 1 开始
size	number	10	每页条数，上限 500，超出自动收敛为 500
orderBy	string	-	排序字段，驼峰或下划线均可（如 <code>createTime</code> ）。仅允许字母、数字、下划线，含非法字符时排序被忽略
asc	boolean	false	是否升序，默认 false（新数据在前）

（2）出参（data 为统一分页结构）

```
{
  "code": 0,
  "success": true,
  "message": "success",
  "data": {
    "content": [ { "id": "1946xxx", "name": "测试客户" } ],
    "total": 57,
```



```
        "size": 10,

        "current": 1,

        "pages": 6,

        "empty": false

    }

}
```

字段	类型	说明
content	array	当前页数数据列表
total	number	总条数
size	number	每页条数
current	number	当前页码（从 1 开始）
pages	number	总页数
empty	boolean	是否空结果（total == 0），前端无需再判断 content.length

2.6 通用业务状态码

错误码分段规则（新业务模块会按段扩展，前端按段兜底处理即可）：

区间	含义
400xx	参数类错误
401xx	认证/身份类错误
403xx	权限类错误
404xx	资源不存在
405xx	请求方式错误
500xx	系统/外部调用错误
6xxxx	业务错误

标准通用状态码列表：

code	含义	前端处理建议
0	成功	-
40001	请求参数缺失或格式错误	展示 message（含具体字段信息）
40002	无效的请求体	展示 message
40101	API 签名验证失败	展示 message
40102	请求时间戳已过期	展示 message
40103	未登录或登录已过期	清除本地 token，跳转登录页
40301	操作权限不足	提示无权限，不跳登录
40401	请求的资源不存在	展示 message
40501	错误的请求方式	检查 GET/POST 是否用反
50001	系统内部错误	提示「系统繁忙，请稍后重试」，报障时附 X-Trace-Id（见 2.9）
50002	外部服务调用失败	同上
60001	通用业务错误	直接展示 message
61001	不支持的登录方式	展示 message
61002	三方授权失败（钉钉 authCode 无效/过期）	提示重新扫码
61003	账号已被禁用	展示 message
-1	未知错误	展示 message

2.7 信封例外：文件导出

Excel 导出类接口不返回 JSON 信封，直接返回二进制流：

- 成功：响应头含 Content-Disposition: attachment;filename=xxx.xlsx（文件名已 URL 编码），响应体为文件流，前端按 blob 接收后触发下载。
- 失败：响应体是 JSON 错误信封（统一结构）。

因此前端处理导出接口时先检测响应的 Content-Type：

- application/json → 按信封解析并提示 message；
- 其他 → 按 blob 下载。

2.8 数据字典

- 字典项分 label / value 两部分：label 是前端展示值（如「官网注册」），value 是存储值（如 "1"）。

提交和回显一律用 **value**, **label** 仅用于展示。

- 下拉框数据源是否走字典接口，以原型标注为准：
 - 原型标注了字典编码(dictCode)的 → 调 GET /api/auth/dict/items?dictCode=xxx 获取 label/value 列表；
 - 是/否、启用/禁用等简单枚举 → 前端直接硬编码，不走字典。

2.9 链路追踪

- 每个响应都带响应头 X-Trace-Id，标识本次请求的全链路日志。
- 前端报障时请附上出错请求的 **X-Trace-Id**，后端可据此直接定位日志。
- 前端也可主动在请求头传 X-Trace-Id（无则后端自动生成）。