认证服务

提供登录/MFA认证等多种认证的服务，所有认证页通过 Web 的方式提供。

【TODO】 认证的安全策略（失败次数锁 uid，锁 ip）

1. API 相关

1. 请求头须包含五个字段，mid(设备ID，**所有接口**)，platform(系统平台，**所有接口**)，ts(时间戳，**所有接口**)，nonce(随机串，**所有接口**)，sign(请求签名，**所有接口**)，domain(当前用户选择的组织域，**拉取组织域不需要**)
2. 服务端会在拉取组织用户域接口根据 mid 生成一个 Cookie(包含 mid 和生成时间)，其他的所有接口全部会检查这个 Cookie，不合法请求会被拒绝
3. ts 检查请求时间是否合法，前后误差不超过**3分钟**
4. nonce 防重放攻击，**3分钟**内不能出现重复
5. sign 检查请求是否合法，考虑到 Webview 有可能被拿到链接直接在浏览器中使用，所以签名中除了要包含 ts 和 nonce，还需要 mid，**sign=Base64(HMAC-SHA256("authkeeper"+ts+body字符串+nonce, mid))**
6. 全部接口请求使用 **POST**，其他方法或是不存在的接口全部返回 404
7. 需要账户密码认证的，密码如果不是一次性（短信/邮件动态口令，OTP 口令），那么密码需要进行加密以满足合规，**en_password=HexEncodeString(SM2(password, public_key))**
8. 所有请求都包含请求 ID，在请求返回的头中，字段对应 AK-Request-ID

2. 接口定义

2.1 拉取用户组织域

- **接口说明：** 【iOA 定制接口】，用于返回所有的用户组织域目录。如果有多个目录，会返回目录列表，包含（目录 ID，目录名称，包含的认证源 ID 列表）；如果只有一个目录，则直接返回对应的登录配置。
- **接口地址：** /authkeeper/api/v1/domains

2.1.1 请求参数（无需）

2.1.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
domains	array of object	否	组织域列表，和下面的 domain 配置二选一
domain_id	string	是	组织域 ID
domain_name	string	是	组织域名称
config_ids	array of string	是	包含的认证源 ID 列表

示例：

- 有多个

```
{
    "code": "Success",
    "message": "",
    "skip": false,
    "domains": [
        {
            "id": "id",
            "name": "name",
            "configs": ["config-id-1", "config-id-2"]
        }
    ]
}
```

2.2 拉取组织域对应的所有登录方式

- **接口说明：** 提供认证源 ID 列表，返回对应的详细配置列表。如果 config_ids 为空，则从头部读取组织域，然后查找对应的认证源。
- **接口地址：** /authkeeper/api/v1/login-configs

2.2.1 请求参数

参数名称	类型	是否必需	描述
config_ids	array of string	否	认证源 ID 列表

请求示例：

```
{
    "config_ids": ["config-id-1", "config-id-2"]
}
```

2.2.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
configs	array of object	否	认证源 ID 列表对应的详细配置信息
id	string	是	认证源 ID
type	string	是	认证源类型
name	string	是	认证源名称
tip	string	是	认证源提示语（iOA 产品需求）
config	object	否	可能需要的相关配置内容，账密/短信/邮件/OTP 类型为空，企业微信为{"schema":"", "corp_id":"", "agent_id":"", "url":""}，钉钉为{"app_key":"", "url":""}，飞书为{"app_id":"", "url":""}，其他 SSO 后续补充，**以上配置的 url 全部用 ${uri} 表示重定向地址，需要前端自行替换**

示例：

```
{
    "code": "Success",
    "message": "",
    "configs": [
        {
            "id": "id",
            "type": "type",
            "name": "name",
            "tip": "tip",
            "config": {
                "xxx": "xxx"
            }
        }
    ]
}
```

2.3 发送短信/邮件

- **接口说明：** 提供手机号/邮箱/UserID，发送短信或邮件。
- **接口地址：** /authkeeper/api/v1/send

2.3.1 请求参数

参数名称	类型	是否必需	描述
config_id	string	是	认证源 ID
uid	string	是	用户名，手机号，邮箱都可以

请求示例：

```
{
    "config_id": "config_id",
    "uid": "手机号 or 邮箱 or UserID"
}
```

2.3.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息

示例：

```
{
    "code": "Success",
    "message": ""
}
```

2.4 登录

- **接口说明：** 登录认证。
- **接口地址：** /authkeeper/api/v1/login

2.4.1 请求参数

参数名称	类型	是否必需	描述
config_id	string	是	认证源 ID
uid	string	是	用户名、邮箱、手机号都塞这个字段，对于 SSO 类型的，可以为空，自建扫码认证填二维码 ID
code	string	是	密码、动态口令、OTP、SSO Code 都塞这个，**如果不是一次性密码，必须 SM2 加密，然后 Base64**
redirect_uri	string	否	飞书和部分 SSO 需要这个字段，重定向的 URI 是前端自己定

请求示例：

```
{
    "config_id": "config_id",
    "uid": "",
    "code": "code",
    "redirect_uri": ""
}
```

2.4.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
need_new_password	bool	是	对于 iOA 自建账号登录，是否需要修改密码
need_mfa	bool	是	是否需要进行二次认证

参数名称	类型	是否必需	描述
domain_id	string	是	用户认证用的组织域
uid	string	是	用户 ID
mid	string	是	设备 ID
device_type	string	是	设备类型
ticket	string	是	iOA 颁发的票据
ticket_type	number	是	iOA 颁发票据的类型
config_ids	array of string	否	二次认证可用的认证源 ID 列表。如果 need_mfa 为 true，则不为空

示例：

```
{
    "code": "Success",
    "message": "",
    "need_new_password": true|false,
    "need_mfa": true|false,
    "domain_id": "domain_id",
    "uid": "uid",
    "mid": "mid",
    "device_type": "type",
    "ticket": "ticket",
    "ticket_type": 0|1|2,
    "config_ids": ["config-id-1", "config-id-2"]
}
```

2.5 拉取当前用户可用的 MFA 认证源配置

- **接口说明：** 提供认证源 ID 列表，返回对应的详细配置列表。
- **接口地址：** /authkeeper/api/v1/mfa-configs

2.5.1 请求参数

参数名称	类型	是否必需	描述
uid	string	是	用户 ID
config_ids	array of string	是	认证源 ID 列表

请求示例：

```
{
    "uid": "UserID",
    "config_ids": ["config-id-1", "config-id-2"]
}
```

2.5.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
configs	array of object	否	认证源 ID 列表对应的详细配置信息
id	string	是	认证源 ID
type	string	是	认证源类型
name	string	是	认证源名称
tip	string	是	认证源提示语（iOA 产品需求）
config	object	否	可能需要的相关配置内容，短信/邮件为{"uid": "xxx"}，uid 为脱敏之后的邮箱或是手机号；企业微信为{"corp_id":"", "agent_id":"", "url":""}，钉钉为{"app_key":"", "url":""}，飞书为{"app_id":"", "url":""}，其他 SSO 后续补充， **以上配置的 url 全部用 ${uri} 表示重定向地址，** **需要前端自行替换**

示例：

```
{
    "code": "Success",
    "message": "",
    "configs": [
        {
            "id": "id",
            "type": "type",
            "name": "name",
            "tip": "tip",
            "config": {
                "xxx": "xxx"
            }
        }
    ]
}
```

2.6 拉取当前用户的挑战认证配置

- **接口说明：** 提供加密压缩后的大票请求数据，拿到对应的挑战认证 ID 列表，使用此接口后，需要继续调用 /authkeeper/api/v1/mfa-configs。
- **接口地址：** /authkeeper/api/v1/challenge

2.6.1 请求参数

参数名称	类型	是否必需	描述
data	string	是	客户端请求 GetStatusTicketV1 的加密压缩后的请求体字符串

请求示例：

```
{
    "data": "encrpted ticket status request data",
}
```

2.6.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
domain_id	string	是	用户认证用的组织域

参数名称	类型	是否必需	描述
uid	string	是	用户 ID
mid	string	是	设备 ID
device_type	string	是	设备类型
ticket	string	是	iOA 颁发的票据
ticket_type	number	是	iOA 颁发票据的类型
config_ids	array of string	是	挑战认证可用的认证源 ID 列表。如果 need_mfa 为 true，则不为空

示例：

```
{
    "code": "Success",
    "message": "",
    "domain_id": "domain_id",
    "uid": "uid",
    "mid": "mid",
    "device_type": "type",
    "ticket": "ticket",
    "ticket_type": 0|1|2,
    "config_ids": ["config-id-1", "config-id-2"]
}
```

2.7 MFA 认证（登录二次认证/挑战认证/内部多因子认证）

- **接口说明：** MFA，支持多个因子同时认证。
- **接口地址：** /authkeeper/api/v1/mfa

2.7.1 请求参数

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
domain_id	string	是	用户认证用的组织域
uid	string	是	用户 ID

参数名称	类型	是否必需	描述
mid	string	是	设备 ID
device_type	string	是	设备类型
ticket	string	是	iOA 颁发的票据
ticket_type	number	是	iOA 颁发票据的类型
actions	array of object	是	认证请求列表
type	string	否	可空，认证类型
config_id	string	是	认证源 ID
uid	string	是	UserID，自建扫码认证填二维码 ID
code	string	是	密码、动态口令、OTP、SSO Code 都塞这个， **如果不是一次性密码，必须 SM2 加密，然后 Base64**
redirect_uri	string	否	飞书和部分 SSO 需要这个字段，重定向的 URI 是前端自己定
order	number	否	保留字段，目前无用。

请求示例：

```
{
    "code": "Success",
    "message": "",
    "domain_id": "domain_id",
    "uid": "uid",
    "mid": "mid",
    "device_type": "type",
    "ticket": "ticket",
    "ticket_type": 0|1|2|3,
    "actions": [
        {
            "type": "type_str",
            "config_id": "config_id",
            "uid": "user_id",
            "code": "code",
            "redirect_uri": ""
        }
    ]
}
```

2.7.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
domain_id	string	否	用户认证用的组织域
uid	string	否	用户 ID
mid	string	否	设备 ID
device_type	string	否	设备类型
ticket	string	否	iOA 颁发的票据
ticket_type	number	否	iOA 颁发票据的类型
results	array of object	是	认证结果列表
type	string	是	认证源类型
config_id	string	是	认证源 ID
result	bool	是	对应的认证源认证结果

参数名称	类型	是否必需	描述
extra	bool	否	保留字段，目前无用。

示例：

```
{
    "code": "Success",
    "message": "",
    "domain_id": "domain_id",
    "uid": "uid",
    "mid": "mid",
    "device_type": "type",
    "ticket": "ticket",
    "ticket_type": 0|1|2,
    "results": [
        {
            "type": "type",
            "config_id": "config_id",
            "result": true|false
        }
    ]
}
```

2.8 检查 TOTP 种子是否超量

- **接口说明：** 检查 OTP 种子是否已达上限。
- **接口地址：** /authkeeper/api/v1/otp/limit

2.8.1 请求参数

参数名称	类型	是否必需	描述
uid	string	是	用户 ID

请求示例：

```
{
    "uid": "user_id"
}
```

2.8.2 返回结果

参数名称	类型	是否必需	描述

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息

示例：

```
{
    "code": "Success",
    "message": ""
}
```

2.9 获取 TOTP 二维码内容

- **接口说明：** 获取 TOTP 二维码内容的接口，二维码由前端生成，**totp_url并不完整，URL 后面还要拼接 &address=xxx，即当前页面的 host，host 需要进行 URLEncode**。此接口会做前置步骤检查，如果二次认证只有 TOTP，那么正常路径下是可以获取到种子，如果不止一个认证方式，那么必须要做 MFA 认证才能够获取种子。
- **接口地址：** /authkeeper/api/v1/otp

2.9.1 请求参数

参数名称	类型	是否必需	描述
uid	string	是	用户 ID

请求示例：

```
{
    "uid": "user_id"
}
```

2.9.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
totp_url	string	否	标准的 OTP URL

示例：


```
{
    "code": "Success",
    "message": "",
    "totp_url": "otpauth://totp/iOA:harold?algorithm=SHA256&digits=6&issuer=iOA&period=30&secret=IJLIFQ
}
```


2.10 自建扫码认证 Polling 接口

- **接口说明：** 获取自建扫码的二维码 ID。如果接口未带二维码 ID，则会生成一个新的二维码，并把状态转为等待扫码；如果带了二维码 ID，则返回当前二维码的状态。由前端生成二维码，二维码要包含二维码 ID。前端要响应对应的二维码状态。
- **接口地址：** /authkeeper/api/v1/qrcode/polling

2.10.1 请求参数

参数名称	类型	是否必需	描述
tmp_id	string	否	二维码 ID，如果没有 ID，则表明要生成一个新的二维码

请求示例：

```
{
    "tmp_id": "qrcode_id"
}
```

2.10.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
tmp_id	string	否	只有新生成二维码才有值
status	string	是	当前二维码的状态，状态见 4

示例：

```
{
    "code": "Success",
    "message": "",
    "tmp_id": "qrcode_id",
    "status": "status"
}
```

2.11 移动端扫码后的页面交互接口

- **接口说明：** 主要是用来改变二维码的状态。
- **接口地址：**
  - 扫码拉起授权页调用：/authkeeper/api/v1/qrcode/scan
  - 授权页点击确认调用：/authkeeper/api/v1/qrcode/confirm
  - 授权页点击取消调用：/authkeeper/api/v1/qrcode/cancel

2.11.1 请求参数

参数名称	类型	是否必需	描述
tmp_id	string	是	扫描的二维码 ID
data	string	是	票据检查接口必须的数据，原样透传

请求示例：

```
{
    "tmp_id": "qrcode_id",
    "data": "ticket_status_data"
}
```

2.11.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息

示例：

```
{
    "code": "Success",
    "message": ""
}
```

2.12 iOA 自建账号修改密码

- **接口说明：** iOA 自建账号登录成功后如果要求修改密码，则需要调用此接口修改密码。新旧密码都需要**SM2**加密，未加密的两个密码不能一样。
- **接口地址：** /authkeeper/api/v1/password

2.12.1 请求参数

参数名称	类型	是否必需	描述
uid	string	是	用户名
old_password	string	是	旧密码，SM2 加密
new_password	string	是	新密码，SM2 加密

请求示例：

```
{
    "uid": "username",
    "old_password": "SM2(old_password)",
    "new_password": "SM2(new_password)"
}
```

2.12.2 返回结果

参数名称	类型	是否必需	描述
code	string	是	返回错误码
message	string	是	错误码对应的错误信息
need_mfa	bool	是	是否需要进行二次认证
domain_id	string	是	用户认证用的组织域
uid	string	是	用户 ID
mid	string	是	设备 ID

参数名称	类型	是否必需	描述
device_type	string	是	设备类型
ticket	string	是	iOA 颁发的票据
ticket_type	number	是	iOA 颁发票据的类型
config_ids	array of string	否	二次认证可用的认证源 ID 列表。如果 need_mfa 为 true，则不为空

示例：

```
{
    "code": "Success",
    "message": "",
    "need_mfa": true|false,
    "domain_id": "domain_id",
    "uid": "uid",
    "mid": "mid",
    "device_type": "type",
    "ticket": "ticket",
    "ticket_type": 0|1|2,
    "config_ids": ["config-id-1", "config-id-2"]
}
```

3. 错误码

考虑到认证服务的敏感性，不能暴露过多的错误信息给到前端，所以只会有如下错误码。

错误码对应返回的 code，描述对应返回的 message

如果需要查看具体错误信息，可以通过返回头的 ak-request-id，然后到服务日志中查询。

错误码	描述
Success	成功
InvalidParameter	请求参数错误
InternalError	服务内部错误
InvalidUID	用户名或密码错误
InvalidDomain	组织域不存在

错误码	描述
AuthFailure	认证失败
SendFailure	发送失败
SendLimit	发送过于频繁，请稍后再试
MaxSecretLimit	可绑定的 OTP 种子超过最大值
EqualPassword	新旧密码相同

4. 自建扫码二维码状态

状态	描述	其他
waiting	等待扫描	新生成未被扫描的状态
expired	过期	失效的，或是已经认证失败的二维码都是这个状态
scanned	已扫描	移动端已经扫描了二维码，此状态的二维码不会被再次扫描成功
confirmed	已确认	移动端授权页已经点击了确认
cancelled	已取消	移动端授权页已经点击了取消
success	认证成功	移动端授权之后，票据校验成功
failure	认证失败	移动端授权之后，票据校验失败

- 二维码不是 **waiting** 状态，则不可再扫描
- 二维码是 **expired/cancelled/failure** 状态，则桌面端要球必须刷新二维码
- 二维码是 **success** 状态，必须立即发起认证请求
- 二维码是 **scanned/confirmed/cancelled/failure/expired** 状态，则桌面端页面要有相应的 UI 响应