

Aizip Phaten XMOS 芯片授权 Key API

接口描述

该接口用于生成或验证设备的授权密钥，用户需提供设备信息及请求时间戳，并根据签名规则验证请求合法性。

接口 URL

POST http://121.4.106.36:9981/phaten/key

请求头

参数	描述
accept	可接受的返回格式，默认为 */*
Content-Type	指定请求体格式，默认为 application/json

请求体参数

以下是请求体需要的 JSON 格式字段：

参数名	类型	必填	描述
chipId	string	是	设备唯一标识符
factory	string	是	厂商信息：XMOS-XU316-Phaten-Phaten
modelVersion	string	是	设备型号及版本号：DNR_m2.0.0_48KHz_11ms_180K_40dB

参数名	类型	必填	描述
reqTimestamp	string	是	请求的时间戳，格式为 ISO8601，如： 2024-12-18T00:00:00.225Z
sign	string	是	签名，用于验证请求的合法性

签名生成规则

签名规则如下：

```
sign = md5(chipId + factory + modelVersion + reqTimestamp + Secret)
```

- chipId：设备唯一标识符
- factory：厂商信息
- modelVersion：设备型号及版本号
- reqTimestamp：请求时间戳
- Secret：服务器预设的密钥（其他途径发送）

签名计算示例（伪代码）：

```
import hashlib

Secret = ""

chipId = "00000000454e31303733000000000004"
factory = "XMOS-XU316-Phaten-Phaten"
modelVersion = "DNR_m2.0.0_48KHz_11ms_180K_40dB"
reqTimestamp = "2024-12-18T00:00:00.225Z"

data = chipId + factory + modelVersion + reqTimestamp + Secret
sign = hashlib.md5(data.encode('utf-8')).hexdigest()
```

示例请求

```
curl -X POST "http://121.4.106.36:9981/phaten/key" \
-H "accept: */*" \
-H "Content-Type: application/json" \
-d '{
  "chipId": "00000000454e31303733000000000004",
  "factory": "XMOS-XU316-Phaten-Phaten",
  "modelVersion": "DNR_m2.0.0_48KHz_11ms_180K_40dB" ,
  "reqTimestamp": "2024-12-18T00:00:00.225Z",
  "sign": "2b9af74f888683e671d9f9b7192a0c099"
}'
```

返回数据格式

成功响应

HTTP 状态码： 200 OK
响应体示例：

```
{
  "code": 200,
  "message": "操作成功",
  "data": {
    "factory": "XMOS-XU316-Phaten-Phaten",
    "chipId": "00000000454e31303733000000000004",
    "modelVersion": "DNR_m2.0.0_48KHz_11ms_180K_40dB",
    "sn": "4474BE0D7A8A346C110BE79AD8324720"
  }
}
```

字段名	类型	描述
code	int	状态码，成功时为 200
message	string	操作结果描述
data.factory	string	厂商信息

字段名	类型	描述
data.chipId	string	设备唯一标识符
data.modelVersion	string	设备型号及版本号
data.sn	string	设备序列号（授权密钥）

更新记录

- **v1.0.1:** 更新返回数据结构及字段说明
- **v1.0.0:** 初版文档发布