# 升级接口

公司内部测试环境

http://172.16.32.101:8082/

1. **批量批量**

## 批量上送出生证接口

url: http://ip:port/api/update/uploadBirthCertBatch

公司测试环境：http://172.16.32.101:8082/api/update/uploadBirthCertBatch

◆请求要素

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** | **是否必须** |
| deviceList | List |  |  | 🟊 |
| - deviceCode | S | 设备编号 |  | 🟊 |
| - birthCert | S | 出生证 | Base64字符串 | 🟊 |

示例：

{

“firmwareId”:”123”,

“deviceList”:[

{“deviceCode”:”90001”,”birthCert”:”出生证base64字符串”},

{“deviceCode”:”90001”,”birthCert”:”出生证base64字符串”},

...

]

}

◆应答要素

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** |
| code | Int | 状态 | 0：正常  1：设备出生证缺失（此时msg未出生证数据异常的设备编号，多个时使用英文逗号分隔）  其他：异常 |
| msg | S | 异常描述（成功时为”操作成功”） |  |
| data | List | 响应数据 |  |
| - deviceCode | S | 设备编号 |  |
| - secretKey | S | 密钥交互结果 |  |

示例：

{

“code”:0,

“msg”:””,

“data”:[

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

...

]

}

## 批量交换密钥接口V1

url: http://ip:port/api/update/secretKeyExchangeBatch

公司测试环境：http://172.16.32.101:8082/api/update/secretKeyExchangeBatch

◆请求要素

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** | **是否必须** |
| firmwareId | S | 固件ID |  | 🟊 |
| deviceList | List |  |  | 🟊 |
| - deviceCode | S | 设备编号 |  | 🟊 |
| - birthCert | S | 出生证 | Base64字符串 | 🟊 |

示例：

{

“firmwareId”:”123”,

“deviceList”:[

{“deviceCode”:”90001”,”birthCert”:”出生证base64字符串”},

{“deviceCode”:”90001”,”birthCert”:”出生证base64字符串”},

...

]

}

◆应答要素

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** |
| code | Int | 状态 | 0：正常  其他：异常 |
| msg | S | 异常描述（成功时为”操作成功”） |  |
| data | List | 响应数据 |  |
| - deviceCode | S | 设备编号 |  |
| - secretKey | S | 密钥交互结果 |  |

示例：

{

“code”:0,

“msg”:””,

“data”:[

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

...

]

}

## 批量交换密钥接口V2

url: http://ip:port/api/update/secretKeyExchangeBatch/v2

公司测试环境：http://172.16.32.101:8082/api/update/secretKeyExchangeBatch/v2

V2版本的变动：上传时，不再上传出生证。出生证以通过上送出生证接口上送。

◆请求要素

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** | **是否必须** |
| firmwareId | S | 固件ID |  | 🟊 |
| deviceCodeList | List | 设备编号 |  | 🟊 |

示例：

{

“firmwareId”:”123”,

“deviceList”:[

”90001”,”90002”,

...

]

}

◆应答要素

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** |
| code | Int | 状态 | 0：正常  1：设备出生证缺失（此时msg为没有出生证数据的设备编号，多个时使用英文逗号分隔）  其他：异常 |
| msg | S | 异常描述（成功时为”操作成功”） |  |
| data | List | 响应数据 |  |
| - deviceCode | S | 设备编号 |  |
| - secretKey | S | 密钥交互结果 |  |

示例：

{

“code”:0,

“msg”:””,

“data”:[

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

{“deviceCode”:”90001”,”secretKey”:”密钥交互结果Hex字符串”},

...

]

}

设备出生证缺失

{

“code”:1,

“msg”:”90001,90002”

}

## 批量上送版本信息接口

url: http://ip:port/api/update/uploadVersionInfoBatch

公司测试环境：http://172.16.32.101:8082/api/update/uploadVersionInfoBatch

◆请求要素

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** | **是否必须** |
| deviceList | List |  |  | 🟊 |
| - deviceCode | S | 设备编号 |  | 🟊 |
| - versionInfo | S | 版本信息 | json字符串  key - value（key是cosType，value是cosVersion） | 🟊 |

示例：

{

“deviceList”:[

{“deviceCode”:”90001”,”versionInfo”:"{\"9531\":\"1.1\",\"324\":\"1\"}"]},

{“deviceCode”:”90002”,”versionInfo”:"{\"9531\":\"1.1\",\"324\":\"1\"}".]},

...

]

}

◆应答要素

|  |  |  |  |
| --- | --- | --- | --- |
| **字段名** | **类型** | **字段含义** | **具体描述** |
| code | Int | 状态 | 0：正常  1：设备版本保存异常（此时msg为版本保存异常的设备编号，多个时使用英文逗号分隔）  其他：异常 |
| msg | S | 异常描述（成功时为”操作成功”） |  |

示例：

{

“code”:0,

“msg”:””

}

# 附录

## 升级证书格式

多个TLV组合，每个T和L域分别占用2字节

|  |  |  |
| --- | --- | --- |
| Tag | Value说明 | 备注 |
| 0001 | 客户号 | 内容转化为Hex字符后，第4-8个字符 |
| 0002 | 预留字段 |  |
| 0003 | 时间 | yyyyMMddhhmmss |
| 0004 | 序号 | 号段限制时，限制的就是这个序号 |
| 0005 | 公钥N | 04+公钥N+公钥E 是验签公钥  验证查询升级接口中的newCosInfo |
| 0006 | 公钥E |
| 0007 | 签名值（签名原文为0001~0006的tlv内容） |  |

## 固件资源内容格式

从固件包中的字段，需要能知道是要给网关或者网关下的哪种设备升级，且升级的是哪种COS。

|  |  |  |
| --- | --- | --- |
| TAG(Hex 1Byte) | LEN(DER) | VAL(LEN Bytes) |
| 70 | XX | |  |  |  |  | | --- | --- | --- | --- | | TAG(Hex 1Byte) | LEN(DER) | VAL(LEN Bytes) | DESC | | 41 | <=16 | 起始序列号(字符串) |  | | 42 | <=16 | 终止序列号(字符串) |  | | 43 | 4 | 客户号(字符串) |  | | 44 | XX | 固件版本信息(字符串) |  | | 45 | 2 | 升级类型(字符串) |  | | 46 | 2 | 版本格式(字符串) |  | | 47 | XX | 固件UUID(字符串) |  | | 48 | XX | 产品名(字符串) |  | | 49 | XX | 固件ID |  |   管理信息 |
| 51 | XX | 固件包信息+签名 |
| 52 | XX | 固件包密钥密文(此部分信息需要传给服务器端的硬件授权Key) |
| 71 | XX | |  |  |  |  | | --- | --- | --- | --- | | TAG(Hex 1Byte) | LEN(DER) | VAL(LEN Bytes) | DESC | | 57 | 2 | 固件包分组数据块长度(客户端按此分组长度分包将密文固件包传入待升级设备) |  | | 58 | 16 | 固件包MAC(此部分数据在所有密文固件包传入待升级设备后传入) |  | | 59 | XX | 密文固件包(应是分组长度整数倍<TAG 57> ) |  |   固件包内容 |