**内 部**

**可信移动安全服务平台与CB对接**

**接口规范**

**二〇二一年十二月**

目录

[1 接口规范 3](#_Toc90884077)

[1.1 技术要求 3](#_Toc90884078)

[1.1.1 数据传输加密机制 3](#_Toc90884079)

[1.1.2 支持扩展性 3](#_Toc90884080)

[1.1.3 容错机制 3](#_Toc90884081)

[1.2 接口规范 3](#_Toc90884082)

[1.2.1 接口设计要求 3](#_Toc90884083)

[1.2.2 接口工作模式 3](#_Toc90884084)

[1.2.3 接口错误处理 4](#_Toc90884085)

[2 接口定义 5](#_Toc90884086)

[2.1 租户开通 5](#_Toc90884087)

[2.1.1 字段详情 5](#_Toc90884088)

[2.1.2 接口详情 6](#_Toc90884089)

[2.2 租户变更 7](#_Toc90884090)

[2.2.1 字段详情 7](#_Toc90884091)

[2.2.2 接口详情 8](#_Toc90884092)

[2.3 租户注销 9](#_Toc90884093)

[2.3.1 字段详情 9](#_Toc90884094)

[2.3.2 接口详情 9](#_Toc90884095)

[2.4 子用户新增 10](#_Toc90884096)

[2.4.1 字段详情 10](#_Toc90884097)

[2.4.2 接口详情 11](#_Toc90884098)

[2.5 子用户变更 11](#_Toc90884099)

[2.5.1 字段详情 11](#_Toc90884100)

[2.5.2 接口详情 12](#_Toc90884101)

[2.6 子用户取消订购 13](#_Toc90884102)

[2.6.1 字段详情 13](#_Toc90884103)

[2.6.2 接口详情 14](#_Toc90884104)

[2.7 子用户状态变化 14](#_Toc90884105)

[2.7.1 字段详情 14](#_Toc90884106)

[2.7.2 接口详情 16](#_Toc90884107)

# 接口规范

## 技术要求

### 数据传输加密机制

由于系统数据的重要性，为了加强传输过程中数据的安全，采用HTTPS协议进行数据传输。

### 支持扩展性

服务采用RESTful的接口实现方式；数据采用JSON格式表示，并且符合相应的JSON Schema；开发语言无绑定要求。

### 容错机制

为保证数据的一致性、可靠性，数据上报服务应支持容错重传机制。

## 接口规范

### 接口设计要求

（1）接口协议均基于HTTP/HTTPS协议，采用RESTful的接口实现方式。

（2）接口调用要求具备认证机制。

（3）数据格式要求统一使用JSON格式表示，并且符合相应的JSON Schema。

（4）报文内容处理须满足事务处理一致性原则。根据JSON名称和路径进行精确定位，不应根据字段的顺序来获取字段值。报文统一采用UTF-8进行编码。单次交互报文大小限制在10MB以内，若大于10MB数据上报方需要进行拆包处理。

（5）错误处理要求保持事物处理一致性，使用统一标准的错误代码。

### 接口工作模式

接口采用推送模式，由CB通过集团能开平台，北分能开平台最终推送到可信平台。推送流程如下图：



推送工作模式好处是信息实时性高。不过需要推送者处理网络错误，当网络异常时，有重传机制。

### 接口安全机制

由于接口在互联网上暴露，应保证通讯双方身份的合法性，通信内容的机密性，且内容无法被篡改。可信平台接口通过服务器和客户端之间的HTTPS双向证书验证保证通讯的安全性。

1. 可信平台为能开平台签发接口调用客户端证书和客户端私钥。
2. 能开平台调用可信平台接口时，应进行HTTP双向证书认证。可信平台会验证能开平台请求中的客户端证书，能开平台也应验证可信平台的服务端证书。

同时，每次请求接口需要携带公共HTTP请求头，具体描述如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 名称 | 类型 | 是否必填 | 说明 |
| appId | string | 是 | 请求方标识，cb服务标识为app\_cb\_service |
| nonce | string | 是 | 请求方产生的随机数字符串 |
| timestamp | string | 是 | 时间戳, epoch毫秒数 |
| sign | string | 是 | 由appId, nonce, timestamp和共享秘钥生成的签名。签名算法见下 |
| import javax.crypto.Mac;  import javax.crypto.SecretKey;  import javax.crypto.spec.SecretKeySpec;  import java.nio.charset.StandardCharsets;  import java.security.InvalidKeyException;  import java.security.NoSuchAlgorithmException;  import java.util.Base64;  public class HmacAuthUtil {      /\*\*       \* @param appId     请求方标识       \* @param appSecret 用户共享秘钥       \* @param nonce     随机数       \* @param timestamp 时间戳       \* @return 签名值base64字符串       \*/      public static String sign(String appId, String appSecret, String nonce, String timestamp) {          SecretKey key = new SecretKeySpec(appSecret.getBytes(StandardCharsets.UTF\_8), "HMAC");          try {              Mac mac = Mac.getInstance("HmacSHA256");              mac.init(key);              String text = appId + nonce + timestamp;              return Base64.getEncoder().encodeToString(mac.doFinal(text.getBytes(StandardCharsets.UTF\_8)));          } catch (NoSuchAlgorithmException | InvalidKeyException e) {              throw new IllegalStateException(e);          }      }  } | | | |

### 接口错误处理

接口调用失败时，需要根据HTTP状态码进行响应处理。

|  |  |  |
| --- | --- | --- |
| 错误类型 | 错误信息 | 错误处理方式 |
| 网络连接超时 | HTTP状态码: 408 | 重新传输。当出现网络问题时，调用者应延迟一段时间，如10分钟，再发起重新传输。 |
| 网络限流 | HTTP状态码: 509 | 重新传输。当出现网络问题时，调用者应延迟一段时间，如10分钟，再发起重新传输。 |
| 数据格式错误 | HTTP状态码: 400  返回json范例：  {  "timestamp":1535539654905,  "status":400,  "error":"Bad Request",  "errors":[  {  "arguments":[  {  "code":"cmcId",  "codes":["orgDto.cmcId","cmcId"],  "defaultMessage":"cmcId"  }  ],  "bindingFailure":false,  "code":"NotEmpty",  "codes":["NotEmpty.orgDto.cmcId","NotEmpty.cmcId",  "NotEmpty.java.lang.String","NotEmpty"],  "defaultMessage":"省份标识不能为空",  "field":"cmcId",  "objectName":"orgDto"  },  {  "arguments":[  {  "code":"data",  "codes":["orgDto.data","data"],  "defaultMessage":"data"  }  ],  "bindingFailure":false,  "code":"NotEmpty",  "codes":["NotEmpty.orgDto.data","NotEmpty.data",  "NotEmpty.java.util.List","NotEmpty"],  "defaultMessage":"机构数据列表不能为空",  "field":"data",  "objectName":"orgDto",  "rejectedValue":[]  }  ],  "message":"Validation failed for object='orgDto'. Error count: 2",  "path":"/mpscmc/v1/ua/org"  } | 调用者应检查数据格式，修改上报程序。并使用正确的格式进行重新上报。 |
| 业务错误 | TODO： |  |

# 接口定义

## 租户开通

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| 租户管理员账号 | tenantAccount | String | 1 | 64 | 是 | 租户管理员账号。为了和运营侧手工创建的账号区分开，可以添加一个前缀，例如cb\_admin1 |
| 租户名称 | tenantName | String | 1 | 64 | 是 |  |
| 所属行业 | industry | String | 1 | 64 | 是 |  |
| 租户联系人邮箱 | contactMail | String | 1 | 64 | 是 |  |
| 租户联系人姓名 | contactName | String | 1 | 64 | 是 |  |
| 租户联系人手机号 | contactMobilePhone | String | 1 | 64 | 是 |  |
| 首次授权终端数量 | licenseDevNum | Integer |  |  | 是 |  |
| 产品资费信息 | priceType | Integer |  |  | 是 | 标准版：30  定制版: 400 |
| 授权截止时间 | licenseEndTime | String |  |  | 是 | 格式yyyy-mm-dd |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /tenant/register |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "tenantAccount": "test\_admin",  "tenantName": "测试租户",  "industry": "其他行业",  "contactMail": "abc@123.com",  "contactName": "张三",  "contactMobilePhone": "11122334455",  "priceInfo": "默认资费",  "licenseDevNum": 200,  "licenseEndTime": ”2021-03-05”,  "actionTime":”2021-03-05”,  "cbAcceptTime":”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 租户变更

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识。租户变更时，必须传递。 |
| 租户联系人邮箱 | contactMail | String | 1 | 64 | 否 |  |
| 租户联系人姓名 | contactName | String | 1 | 64 | 否 |  |
| 租户联系人手机号 | contactMobilePhone | String | 1 | 64 | 否 |  |
| 产品资费信息 | priceType | Integer |  |  | 否 | 标准版：30  定制版: 400 |
| 授权终端数量 | licenseDevNum | Integer |  |  | 否 | 该字段表示租户授权终端数的最终值 |
| 授权截止时间 | licenseEndTime | String |  |  | 否 | 格式yyyy-mm-dd |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /tenant/update |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "contactMail": "abc@123.com",  "contactName": "张三",  "contactMobilePhone": "11122334455",  "priceInfo": "默认资费",  "licenseDevNum": 200,  "licenseEndTime": ”2021-03-05”,  "actionTime": ”2021-03-05”,  "cbAcceptTime": ”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 租户注销

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /tenant/cancel |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "actionTime": ”2021-03-05”,  "cbAcceptTime": ”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 子用户新增

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 所在租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| 子用户手机号 | mobilePhone | String | 1 | 64 | 是 | CB侧用户唯一标识。可信移动安全平台中，手机号作为用户账号,应具有全局唯一性 |
| 手机号使用人姓名 | name | String | 1 | 64 | 是 |  |
| IMSI | imsi | String | 1 | 64 | 是 |  |
| 子用户资费信息 | userPriceType | Integer |  |  | 是 | 标准版：30、25、20、15、12及10  定制版: 400、300、250、200、150、100及50 |
| ICCID | iccid | String | 1 | 64 | 是 |  |
| 资费生效时间 | actionTime | String |  |  | 是 | 格式yyyy-mm-dd |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /user/register |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "mobilePhone": "11122334455",  "name": "张三",  "imsi": "11122334455",  "iccid": "11122334455",  "actionTime": ”2021-03-05”,  "cbAcceptTime": ”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 子用户变更

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 所在租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| 子用户手机号 | mobilePhone | String | 1 | 64 | 是 | CB侧用户唯一标识。可信移动安全平台中，手机号作为用户账号，应具有全局唯一性 |
| 手机号使用人姓名 | name | String | 1 | 64 | 否 |  |
| 子用户资费信息 | userPriceType | Integer |  |  | 否 | 标准版：30、25、20、15、12及10  定制版: 400、300、250、200、150、100及50 |
| 资费生效时间 | actionTime | String |  |  | 否 | 格式yyyy-mm-dd |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /user/update |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "mobilePhone": "11122334455",  "cbStatus": 0,  "name": "张三",  "imsi": "11122334455",  "iccid": "11122334455",  "actionTime": ”2021-03-05”,  "cbAcceptTime": ”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 子用户取消订购

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 所在租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| 子用户手机号 | mobilePhone | String | 1 | 64 | 是 | CB侧用户唯一标识。可信移动安全平台中，手机号作为用户账号，应具有全局唯一性 |
| 资费失效时间 | stopTime | String |  |  | 是 | 格式yyyy-mm-dd |
| CB受理时间 | cbAcceptTime | String |  |  | 是 | 格式yyyy-mm-dd |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 是 |  |
| 业务流水号 | cbBussNum | String | 1 | 64 | 是 | CB侧工单唯一标识 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /user/cancel |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "mobilePhone": "11122334455",  "imsi": "11122334455",  "iccid": "11122334455",  "actionTime": ”2021-03-05”,  "cbAcceptTime": ”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

## 子用户状态变化

### 字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 备注 |
| 所在租户ID | tenantId | String | 1 | 64 | 是 | CB侧租户唯一标识 |
| 子用户手机号 | mobilePhone | String | 1 | 64 | 是 | CB侧用户唯一标识。可信移动安全平台中，手机号作为用户账号，应具有全局唯一性 |
| 子用户状态 | cbStatus | Integer |  |  | 是 | 0：正常 (子用户创建后默认为正常状态)  1：补/换卡  2：欠费停机  0：欠费复机（状态码和正常一致）  3：欠费销号  4：携号转网 |
| IMSI | imsi | String | 1 | 64 | 否 | 仅在补/换卡时，需要传递。其他场景不需要传递。 |
| ICCID | iccid | String | 1 | 64 | 否 | 仅在补/换卡时，需要传递。其他场景不需要传递。 |
| CB受理时间 | cbAcceptTime | String | 1 | 64 | 否 | 格式yyyy-mm-dd。仅在补/换卡时，需要传递。其他场景不需要传递。 |
| 受理人账号 | cbOperatorAccount | String | 1 | 64 | 否 | 仅在补/换卡时，需要传递。其他场景不需要传递。 |
| 业务流水号 | cbBussNum | String | 1 | 64 | 否 | CB侧工单唯一标识。仅在补/换卡时，需要传递。其他场景不需要传递。 |

### 返回字段详情

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 最小长度 | 最大长度 | 必选 | 说明 |
| 结果代码 | code | Integer |  |  | 是 | 0: 成功 |
| 结果描述 | message | String | 1 | 200 | 是 | 对请求结果的英文描述 |

### 接口详情

|  |  |
| --- | --- |
| URL | /cb\_sync /user/status/update |
| 方法 | POST |
| 参数范例 | {  "tenantId": "12345",  "mobilePhone": "11122334455",  "cbStatus": 1,  "imsi": "11122334455",  "iccid": "11122334455",  "cbAcceptTime":”2021-03-05”,  "cbOperatorAccount": "test\_account",  "cbBussNum": "cb123456",  …  } |
| 正常返回值 | HTTP 200  {     "code": 0,     "message": "ok" } |
| 业务错误返回值 | 待定义 |
| 备注 |  |

# 信息加密存储

可信平台记录的个人信息中的敏感信息需加密保存，包括用户手机号，证件号码，密码，职务和职级。对于存储在MySQL中的数据，采用AES加密算法，密钥长度128位，加密模式为ECB。

## 租户信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 存储介质 | 加密方式 |
| 租户联系人手机号 | contactMobilePhone | String | MySQL | AES |

## 用户信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 数据项名称 | 数据项英文名 | 类型 | 存储介质 | 加密方式 |
| 子用户手机号 | mobilePhone | String | MySQL | AES |