云闪付 APP 内容与用户共享
对接改造指引

1、 前言

按照人行“三个统一”的要求，通过云闪付 App 开放平台，实现云闪付 App 内容快捷、灵活地输出，推动商业银行与云闪付用户互信，为商业银行 App 提供“统一体验、统一标识、统一接口标准”的支付与营销能力提升统一战线的整体竞争力。

商业银行 App 可通过 H5 的方式接入云闪付 App 内容输出的相关业务。

支持的银行移动端渠道包括：总行/分行手机银行。

2、 功能说明

银行移动端渠道接入云闪付 App 内容输出业务时，银行移动端调用云闪付 App 所提供的接口，将银行移动端用户识别 ID、接入方 ID、签名、时间戳、随机字符串等关键信息送至云闪付 APP 后台，查找已关联的云闪付 App 账户，并以该账户登录，以便用户使用云闪付 App 输出的相关服务。

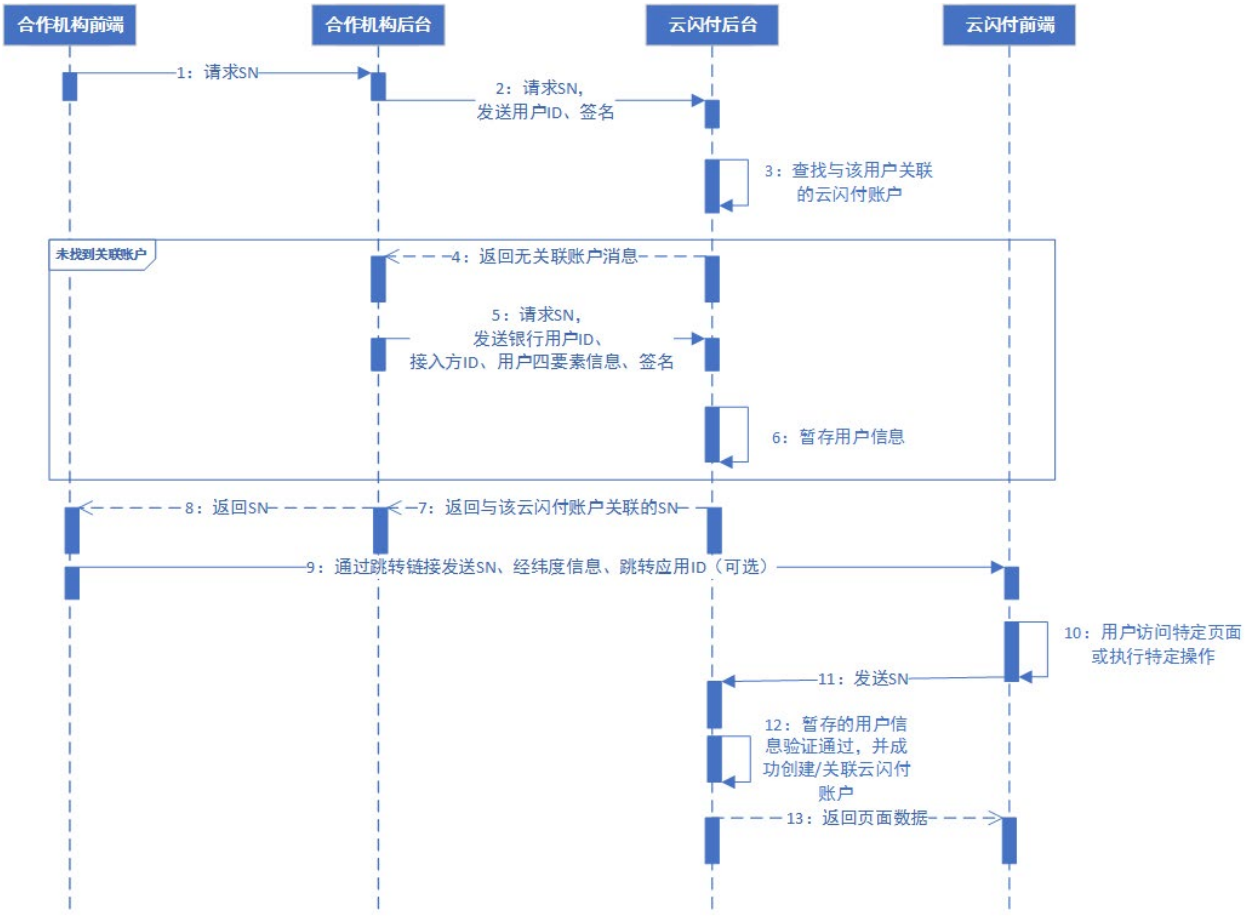
若不存在已关联的云闪付账户，则按照云闪付 App 提供的接口规范，银行移动端需提供应用 ID，用户识别 ID、持卡人的全卡号列表、手机号、姓名、证件号、时间戳、随机字符串等关键信息，云闪付

App 将使用这些信息进行关联/创建云闪付 App 账户，以方便用户使用云闪付 App 输出的相关服务。

为了保障数据传输的安全性，需要双方进行加密传输。

3、流程说明

商业银行 App 通过 H5 的方式接入云闪付 App 内容输出的相关业务的流程说明如下：



流程说明：

1) 银行前端请求银行后台；

2) 银行后台按接口规范（参考本文档第 5、6 章）将用户 ID 及其他所需数据拼装成报文，调用银联后台 findUser（查找用户）接口

提交；

3) 银联后台解析报文，查找该银行上送的用户 ID 是否已关联云闪 App 账户。若未关联进入步骤（4）；若已关联进入步骤（6）；

4) 银联后台将未找到关联用户的消息返回给银行后台；

5) 银行后台将用户识别 ID、持卡人的全卡号列表、手机号、姓名、身份证号及其他所需数据拼装成报文,调用银联后台 bindUser(绑定用户）接口提交；

6) 若找到与银行移动端用户识别 ID 关联的云闪付账户，生成与该云闪付账户关联的 SN 流水号；若未找到与银行移动端用户识别 ID 关联的云闪付账户，则银联后台解析银行后台上送的报文并暂存用户信息数据，生成与该暂存用户信息关联的 SN 流水号；

7) 银联后台将 SN 流水号返回给银行后台

8) 银行后台将获得的 SN 流水号返回给银行前端；

9) 银行前端使用 GET 方式跳转银联 H5 页面，将 SN 流水号（一次有效）、应用 Id 和当前设别的经纬度信息作为参数传递给银联前端。

10) 当用户使用需登录才能使用的相关功能时，触发银联前端 SN 流水号、应用 Id 发送至银联后台；

11) 银联前端将 SN 流水号、应用 Id、是否强制登录标识发至银联后台；

12) 用与 SN 流水号关联的暂存用户信息/云闪付账户，按照云闪付内部逻辑规则完成用户登录；

13) 登录完成后，银联后台将相关页面数据返回至银联前端；

4、数据内容

1）**接入方 ID。**由云闪付 App 为接入机构分配，银行端需要上送接入方 ID，云闪付 App 将根据接入方 ID 筛选与之相关的内容和业务信息，以展示在 H5 页面中。

2）**全卡号列表。**银行端按上送持卡人在银行移动端绑定的本行全卡号列表，云闪付 App 将卡绑定至该持卡人的云闪付 App 账户中，并尝试为卡列表中第一张卡开通快捷支付。

注意：此处卡号可为多个，如传递的卡号为多个，则使用“|”分隔；另外，此处的全卡号即为银行卡上的卡号，不能包含掩码（*）等非卡号的内容。

只可上送银联卡，包括双标卡和单标卡。暂不支持绑定其他卡组织单标卡。

3）**账户类型。**可选字段，银行端上送持卡人银行卡号，区分上送的银行卡类型：01 - 为 I 类户、02 - 为 II 类户、03 - 为III类户，若为空，默认全部为一类账户。

注意：若上送的卡号有多个，则使用“|”分隔各卡号对应的账户类型，排序与全卡号列表排序一一对应。

4）**手机号。**银行端需要上送预留手机号，以便为用户开通/关联云闪付 App 账户。

5）**姓名。**银行端上送预留姓名，以便为用户开通/关联云闪付 APP 账户，快速使用云闪付 APP 输出的相关服务，无需持卡人再前往云

闪付 App 中进行实名认证。

6) **证件类型。**可选字段，银行端需要上送持卡人的证件类型：01 - 身份证；03 - 护照；04 - 回乡证；05 - 台胞证。若为空，默认为身份证。

7) **证件号。**银行端需要上送持卡人的证件号，与证件类型匹配出现以便为用户开通/关联云闪付 APP 账户，快速使用云闪付 App 输出的相关服务，无需持卡人再前往云闪付 App 中进行实名认证。

注意：此处的证件号为持卡人证件上的号码（身份证、护照、回乡证、台胞证），不能包含掩码（*）等其他非证件号的内容。

8) **用户识别 ID。**银行端必须上送银行侧系统中的用户唯一识别 ID，以便云闪付 App 侧的用户 ID 进行绑定关联。

9) **时间戳。**银行端上送报文中含有时间戳，云闪付服务端收到报文时与当前时间进行比较，若超出一定范围（有效期 5 分钟）则抛弃处理，防止重放攻击。

注意：时间戳为从1970年1月1日00:00:00至今的秒数,即当前的时间，单位为秒。

10) **随机字符串。**用于参与签名，如何生成随机字符串详见第 5 章。

11) **渠道名称。**银行端需要上送接入钱包的渠道名称，如：银行客户端、银行微信公共号等。定义如下：1-银行 APP；2-银行公众号。

12) **SN 流水号。**银联后台解析并校验报文后，返回唯一 SN 流水号，用于前台跳转银联页面的传入参数，一次有效，且有效期 30 分钟。

13） **经纬度。**银行端上送当前用户设备的经纬度信息，作为银行前台跳转银联页面的传入参数，用于筛选用户当前所在城市的优惠信息。

注意：跳转链接中加入经纬度参数，如：

lat=31.1111&lon=121.1111

14）**应用Id。**可选参数，若需要跳转至指定应用，则银行端需上送当前的应用Id，作为银行前台跳转银联页面的传入参数。不传则打开服务窗，传递的参数不存在也默认打开服务窗。

注意：跳转链接中加入应用id参数，如：

applicationId=a5949221470c4059b9b0b45a90c81527

5、安全机制

1）利用 symmetricKey 对称密钥对敏感字段加密保护

银行方生成对称密钥（双倍长 3DES），用于敏感数据加密保护。此对称密钥为一次一密,通过银联方给出的公钥（2048bit）加密后按 base64 格式出现在报文中。

使用对称密钥对如下传输内容进行加密保护：**全卡号、账户类型、手机号、姓名、证件类型、证件号**。加密时采用 UTF-8 字符编码，并按 base64 格式出现在报文中。

注意：

- 对报文内容加密时，只对每个字段的 value 值加密，key 值保持不变。例如字段"cardNo":"123456789"，加密后为"cardNo":"M4YRj9sO+Eq1xJnvs1CUZ==";
- 3DES 加密使用的模式为 DESede/ECB/PKCS5Padding。

2）随机字符串生成

随机字符串长度为 16 位，可参考如下实现

```
public static String createNonceStr(int length) {
    String sl = "abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789";
    StringBuilder bf = new StringBuilder();
    for (int i = 0; i < length; i++) {
        bf.append(sl.charAt(new Random().nextInt(sl.length())));
    }
    return bf.toString();
}
```

3）报文的签名机制

将所有待签名参数（除 symmetricKey 外其余字段均参与签名、字符编码为 UTF-8）按照字段名的 ASCII 码从小到大排序（字典序）后，使用键值对的格式（即 key1=value1&key2=value2…）拼接成字符串 string1。

对拼接字符串 string1 进行 RSA 签名后，按 base64 格式出现在报文中。

- value 值无需进行 url 转义
- RSA 签名使用的加密模式为 SHA256WithRSA。

4）报文的通讯协议

使用 https Post 提交、utf-8 字符编码、contentType 为 application/json；银行端上送的报文格式为 json。

示例：

POST … HTTP/1.1

Accept-Language:zh-cn

/***空行***/

……

Content-Length: …

{"appId":"a5949221470c4059b9b0b45a90c81527","timestamp":"1528700527","nonceStr":"AeIku3jje7L1Ys41","cardNo":"xExFz8ISXOqFRUCKgBA==","mobile":"M4YRj9sO+Eq1xJnvs1CUZ==","certifId":"fwoIAhBLsPxww+TuQG/u==","indUsrId":"782d4445fa6d6969","realNm":"9sO+Eq1xJnvs1CUZUOWS/sE==","chnl":"1","signature":"aBHPJm+HQdcm82dgHJPJBdorrT3Mqb3hQz/C6cIfDVOFG+ZJfniB4KPCXioPr2uxKpeOjktvVP5LXOOC7RpQGezqE59kHSPXc69uRV9LM4YRj9sO+Eq1xJnvs1CUZUOWS/sEGxl4XMlHC4bYgT8PPvj3Hej3btmBgNz/lcphbfQ9NGp5T4q1Igl7BMngEDKEktDKH7sDI6wOPu3eqPz+rowFEiuiaHrxuQjymqkV12ifwoIAhBLsPxww+TuQG/una7m6V8V4XnornFlHrb/VjeWGqCGSy/bAZAYlnJcWq99nqKR+Nv1MCEp3Oz4K8mrRtdQxExFz8ISXOqFRUCKgBA==","symmetricKey":"V2fG5IY/qwOBjOiiBmWzOCKLqojzgL9ZO1e4ULpyWi14TAjItAkfnL32+hxeMA+d1ObUhv1rFm3OFGvmvO0NqGig+MfKAqgWvAN84mbCIPaMx8IRpsgxHcOy5IbcXeYC+zfGqPHKLHpvxWVNsESp8LyM+1gguo8/vKVGViZUJtDx1NopucsTOZ4OyvlGQFWOKOEU/CXIx4qlxdxD3YEDVLKbux19IlbshImXebbifOaOAPgJ4ZI7yAbZv/aLu17QVoPjCuClcQU15N27dRET4MmSER9kp/xGj/xr

NAzJ6vxOnfXVefYG9fKTXTCqmnKgk5QfsGVhuQOx+H6+F5gRog=="}（注：此处为报文格式，并非有效数据）

银联端返回的报文格式同为 json，编码 UTF-8,会将银联后台生成的流水号 SN 放入 params 中。如果 resp=00,表示成功返回，SN 为生成的流水号。

示例：

POST … HTTP/1.1

Accept-Language:zh-cn

……

/***空行***/

……

Content-Length：…

{"resp":"00","msg":"","params":{"sn":"546ef50659194ec5a050c07e4396c8b7"}}

（注：此处为报文格式，并非有效数据）

6、报文接口规范

6.1、 findUser-查找用户

1）应用场景实例

该接口用于银行接入云闪付内容输服务后，用户每次通过银行端进入云闪付输出的页面时，银行端以用户识别 ID 查询该用户在云闪付 APP 中是否已有关联的账户。

2）API 调用说明

接口名称	findUser
请求方式	POST
返回结果格式	JSON

3）输入参数

以下表格列出的内容需要组装成 json 格式

名称	类型	是否可选	说明
appId	String	必填	应用 ID，由云闪付 APP 为接入机构分配。
indUsrId	String	必填	用户识别 ID
nonceStr	String	必填	随机字符串
timestamp	String	必填	时间戳
chnl	String	选填	渠道名称,1-银行 APP；2-银行公众号
signature	String	必填	签名

4）返回结果

名称	类型	说明
sn	String	银联后台解析并校验报文后，如用户已关联，则返回唯一 SN 流水号，用于前台跳转银联页面的传入参数
resp	String	银联后台解析并校验报文后，返回的请求结果。00-成功

6.2、 bindUser - 绑定用户

1) 应用场景实例

该接口用于银行在使用 findUser 接口后，若未找到关联的云闪付账户，将用户信息上送，以完成银行端用户账号与云闪付 APP 用户账号关联或创建新的云闪付 APP 账户。

2) API 调用说明

接口名称	bindUser
请求方式	POST
返回结果格式	JSON

3) 输入参数

以下表格列出的内容需要组装成 json 格式

名称	类型	是否可选	说明
appId	String	必填	应用 ID。由云闪付 APP 为接入机构分配。
accType	String	选填	账户类型：01 - 为 I 类户、02 - 为 II 类户、03 - 为III类户，若为空，默认全部为 I 类账户。 若上送的卡号有多个，则使用“|”分隔各卡号对应的账户类型，排序与全卡号列表排序一一对应。 使用 symmetricKey 对称加密，内容为 base64 格式
cardNo	String	选填	银行卡号,银行端必须要上送全卡号，以便持卡人使用云闪付相关服务，此处卡号可为多个，如传递的卡号为多个，则使用“|”分隔；另外，此处的全卡号即为银行卡上的卡号，不能包含掩码（*）等非卡号的内容。 使用 symmetricKey 对称加密，内容为 base64 格式

mobile	String	必填	手机号，使用 symmetricKey 对称加密，内容为 base64 格式
realNm	String	必填	银行端预留姓名，使用 symmetricKey 对称加密，内容为 base64 格式
certType	String	选填	证件类型：01 - 身份证；03 - 护照；04 - 回乡证；05 - 台胞证，默认不填写认为是身份证。使用 symmetricKey 对称加密，内容为 base64 格式
certifId	String	必填	证件号，使用 symmetricKey 对称加密，内容为 base64 格式
indUsrId	String	必填	用户识别 ID
nonceStr	String	必填	随机字符串
timestamp	String	必填	时间戳
chnl	String	选填	渠道名称,1-银行 APP；2-银行公众号
signature	String	必填	签名
symmetricKey	String	必填	3DES 对称密钥 key

4）返回结果

名称	类型	说明
sn	String	银联后台解析并校验报文后，返回唯一 SN 流水号，用于前台跳转银联页面的传入参数
resp	String	银联后台解析并校验报文后，返回的请求结果。00-成功

6.3、 返回报文格式

1）正常请求返回

a） {"msg":"","params":{},"resp":"00"}

b) {"msg":"","params":{"sn":"546ef50659194ec5a050c07e4396c8b7"},"resp":"00"}

2) 异常请求返回

a) {"msg":"系统繁忙，请稍候再试","resp":"00000002"}

b) {"msg":"请求报文解析错误","resp":"01"}

7、 测试联调

功能正式上线前，应完成开发联调和测试，测试环境接口和跳转链接参见下文。

7.1、 测试接口 URL

1) findUser

http://101.231.204.80:8086/app/access/bank/findUser

2) bindUser

http://101.231.204.80:8086/app/access/bank/bindUser

3) 前台云闪付服务窗跳转 URL

http://202.101.25.188:10533/s/open/outApp/react/index.html#/?sn=真实数据&lat=真实数据&lon=真实数据

8、 生产接口地址

1）、findUser

https://wallet.95516.com/app/access/bank/findUser

2）bindUser

https://wallet.95516.com/app/access/bank/bindUser

3）前台云闪付服务窗跳转 URL

https://open.95516.com/s/open/outApp/react/index.html#/?sn= 具体参数值&lon=具体参数值&lat=具体参数值