银联一窗办平台服务商密钥 Rnd 申请指引

服务商在银联一窗办门户完成注册或存量服务商迁移银联一窗办平台之后(可参见注册或迁移指引），可以申请银联服务商密钥。

服务商可以在"银联一窗办平台"(https://pcs.unionpay.com/ycb/pcweb/index.html)搜索栏中搜索"服务商"，选择"服务商 PID 密钥管理"点击"立即办理"。（下图 1 ），然后根据页面引导登录(已注册服务商)或完成注册后可以申请服务商密钥(申请页面见下图 2)。

图 1，通过搜索找到 PID 密钥管理入口

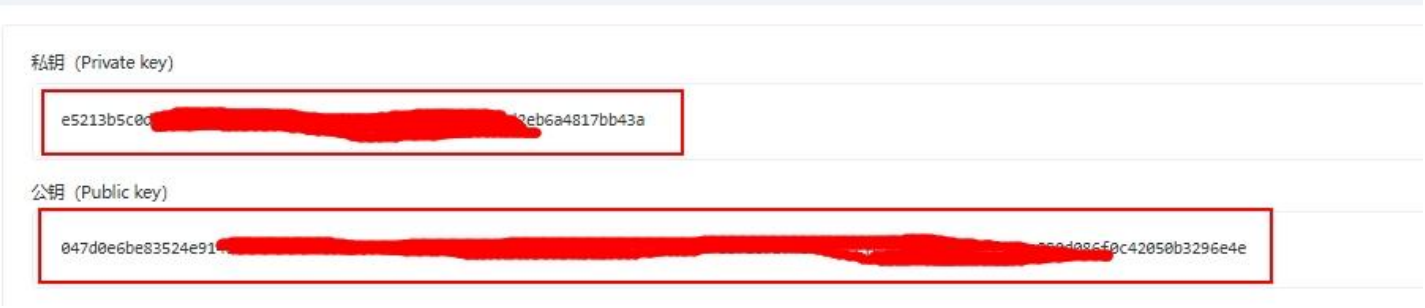
图 2，银联一窗办平台服务商密钥申请页面

如图 2： 服务商申请密钥过程中需使用一对自己的公私钥对，根据银联指定的算法（SM2 算法）对已经获取的服务商身份标识（即 PID，C100XXXX 格式的八位机构代码）进行加密，待银联系统解密核验通过后会为服务商立即分配密钥 Rnd。

其中最关键的服务商公私钥对的生成参考算法和生成步骤如下：

第一步：生成公私钥对

https://btool.cn/sm2-key-generator



第二步：签名

将第一步生成的私钥放入下图的私钥表单中，其他按照下图中的文字描述操作。

https://btool.cn/sm2-sign

第三步，将第一步中的 16 进制"公钥"字符串转为 base64 格式（hex->base64），将第 2 步中的 16 进制的"签名结果"转为 base64 格式（hex->base64）， 然后分别填入上图 2 的服务商秘钥申请网页中的公钥和签名表单中。

其中：hex 到 base64 的转换算法可参考 https://base64.guru/converter/encode/hex

第四步，将申请到的服务商"密钥 Rnd"，通过以下网址解密验证，获取服务商对称密钥

https://tool.hiofd.com/sm2-decrypt-online/

最后：上述指南中的非对称密钥是在第三方网站上生成的，截图中的标注仅供参考，主要用于描述签名过程中的一些算法逻辑。各服务商在投产环节所使用的密钥务必在自己的生产环境中实现生成、签名、解密等步骤，避免密钥信息泄露。