服务商机构标识码信息保护技术方案

本方案包含服务商密钥获取、服务商代码加密、报文传输、密文比对等过程。

一、服务商密钥获取

服务商密钥获取流程图如下:

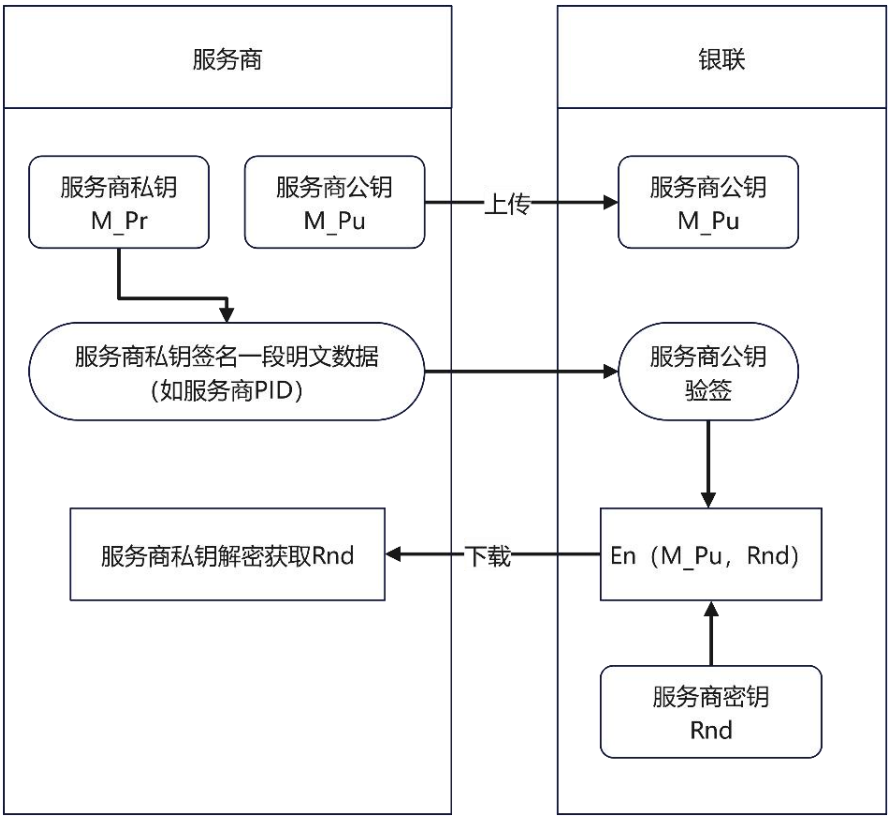

图 1 服务商密钥获取流程图

服务商在服务商合作伙伴平台或银联一窗办平台等对外门户网站上传服务商公钥 M_Pu，生成算法为 SM2，同时使用私钥 M_Pr 签名一段明文数据（如服务商 PID），将签名数据一并上传。银联使用厂商提供的公钥 M_Pu 对签名数据验签，将解密后的结果与服务商 PID 作比对，如信息比对通过，

则认为服务商公钥信息可信；如信息比对不一致，则说明公钥信息已被修改，要求服务商重新生成上传。

比对通过后，银联为当前服务商生成一组 16 个字节、128 位的对称密钥 Rnd（以下称为：数据密钥），使用服务商公钥 M_Pu 做加密。服务商通过合作伙伴平台加密后的数据密钥，并使用私钥 M_Pr 解密获得原始数据密钥 Rnd。在生成数据密钥 Rnd 时，使用服务商代码开展密钥离散，增强数据密钥 Rnd 的随机性。

二、服务商代码加密

（一）随机因子组成

密文数据 SCT 由 PID 明文组合随机因子后使用数据密钥 Rnd 加密后生成，随机因子为服务商订单编号+订单金额，字段定义如下：

字段名称	数据格式	取值规范
服务商订单编号	AN..40	不超过 40 字节的变长字母和/或数字字符，不能含“-”或“_”；由服务商自定义生成，建议全局不重复（例如可将日期时间作为订单编号的一部分），以便后续作为对账依据。
订单金额	N 1..12	长度为 1-12 字节的变长整数值

在开展加密运算时，服务商 PID 代码长度为 11 位，左对齐，右补空格；服务商订单编号长度为 40 位，左对齐，右补空格；订单金额长度为 12 位，以分为单位，右对齐，左补 0。

（二）加密算法

将待加密的数据内容（服务商 PID 明文+随机因子）组

合形成 MAC ELEMEMENT BLOCK（MAB），将 MAB 按每 16 个字节分为一组（如最后一组不足 16 个字节，则右补“0X00”），用数据密钥 Rnd 作为 SM4 密钥进行加密运算，获得 8 字节加密数据 SCT，密文计算过程可参考附录 A。

三、报文传输

在交易报文中**新增服务商信息复合域**，子域信息包括**订单编号、密文数据 SCT** 及未来预留扩展信息。

四、密文比对

在验证服务商 PID 时，银联相关加密平台采用相同的加密算法获得密文数据，与服务商在交易报文中上送的密文数据 SCT 作比对。

五、风险管理

一是需要参考中国银联密钥管理相关要求，对服务商密钥 Rnd 设置有效期（如 5 年），要求定期更新。对于超过有效期的密钥，及时提醒服务商重新申请下载获取。

二是加强对服务商的风险管理，要求服务商在后台系统妥善存储服务商密钥，如采取金融数据加密机等硬件设备。银联侧相关平台设置同时有效密钥的数量上限 N（取值为 2），旧密钥的持续有效期 T（取值为 72 小时）。

附录 A 服务商代码标识加密算法

a) 将（服务商PID+订单编号+订单金额）形成MAC ELEMEMENT BLOCK（MAB）。

b) SM4算法的MAB，按每16个字节做异或，如果最后不满16个字节，则添加“0X00”。

示例：

MAB = M1 M2 M3 M4

其中：

M1 = MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

M2 = MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS31 MS32 MS33 MS34 MS35 MS36

M3 = MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

M4 = MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

按如下规则进行异或运算：

MS01 MS02 MS03 MS04 MS05 MS06 MS07 MS08 MS09 MS10 MS11 MS12 MS13 MS14 MS15 MS16

XOR）

MS21 MS22 MS23 MS24 MS25 MS26 MS27 MS28 MS29 MS30 MS30 MS32 MS33 MS34 MS35 MS36

RESULT BLOCK1 = TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

进行下一次异或

TM01 TM02 TM03 TM04 TM05 TM06 TM07 TM08 TM09 TM10 TM11 TM12 TM13 TM14 TM15 TM16

XOR）

MS41 MS42 MS43 MS44 MS45 MS46 MS47 MS48 MS49 MS50 MS51 MS52 MS53 MS54 MS55 MS56

RESULT BLOCK2 = TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

再进行一次异或运算

TM21 TM22 TM23 TM24 TM25 TM26 TM27 TM28 TM29 TM30 TM31 TM32 TM33 TM34 TM35 TM36

XOR）

MS61 MS62 MS63 MS64 MS65 MS66 MS67 MS68 MS69 MS70 MS71 MS72 MS73 MS74 MS75 MS76

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

c) 将异或运算后的最后16个字节（RESULT BLOCK）转换成32个HEXDECIMAL：

RESULT BLOCK = TM41 TM42 TM43 TM44 TM45 TM46 TM47 TM48 TM49 TM50 TM51 TM52 TM53 TM54 TM55 TM56

= TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082 || TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

d) 取前16个字节用SM4加密：

ENC BLOCK1 = SM4K （TM011 TM012 TM021 TM022 TM031 TM032 TM041 TM041 TM051 TM052 TM061 TM062 TM071 TM072 TM081 TM082）

= EN011 EN012 EN021 EN022 EN031 EN032 EN041 EN042 EN051 EN052 EN061 EN062 EN071 EN072 EN081 EN082

e) 将加密后的结果与后16个字节异或：

EN011 EN012 EN021 EN022 EN031 EN032 EN041 EN042 EN051 EN052 EN061 EN062 EN071 EN072 EN081 EN082

XOR）TM091 TM092 TM101 TM102 TM111 TM112 TM121 TM122 TM131 TM132 TM141 TM142 TM151 TM152 TM161 TM162

TEMP BLOCK=TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16

f) 用异或的结果TEMP BLOCK 再进行一次SM4密钥算法运算。

ENC BLOCK2 = SM4K（TE01 TE02 TE03 TE04 TE05 TE06 TE07 TE08 TE09 TE10 TE11 TE12 TE13 TE14 TE15 TE16）

= EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

g) 将运算后的结果（ENC BLOCK2）转换成32个HEXDECIMAL：

ENC BLOCK2 = EN21 EN22 EN23 EN24 EN25 EN26 EN27 EN28 EN29 EN30 EN31 EN32 EN33 EN34 EN35 EN36

= EN211 EN212 EN221 EN222 EN231 EN232 EN241 EN242 EN251 EN252 EN261 EN262 EN271 EN272 EN281 EN282 ||

EN291 EN292 EN301 EN302 EN311 EN312 EN321 EN322 EN331 EN332 EN341 EN342 EN351 EN352 EN361 EN362

ENC RESULT

= %H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84%H84, %H56, %HB1, %HCD, %H5A, %H3F, %H84, %H84

转换成32个HEXDECIMAL：“8456B1CD5A3F84848456B1CD5A3F8484”

h) 取前8个字节“8456B1CD”作为服务商代码加密数据。

中国银联技术部支持热线

021-20638576

wangchenxi@unionpay.com