交行密码键盘国密改造-验证方案

目　　录

1 国密方案说明.....3

2 国际 RSA 方案说明.....4

3 测试数据.....5

3.1　国密测试数据.....5

3.2　国际测试数据.....5

4　新老加密方案交叉使用说明.....7

5　方案验证时间、地点.....8

1 国密方案说明

1、前端获取密码键盘生成非对称算法 SM2 公钥对主密钥进行公钥加密，将加密数据下发密码键盘;

2、密码键盘用非对称算法 SM2 私钥对主密钥密文进行解密获取主密钥明文;(设备只存储一组主密钥)

3、前端采用主密钥对工作密钥明文进行对称算法 SM4 加密，将工作密钥密文下发密码键盘;(设备只存储一组工作密钥)

4、密码键盘进行 pinblock，采用对称算法 SM4 对 pinblock 进行加密,返回密码密文;

5、前端进行密码密文解密;

注:

PIN 加密算法说明：

密码： 123456
账号： 6220201234567890123
SM4 ZPK 密钥明文： 1234567890ABCDEF1111111111111111

第一步，填充 PIN（2 位长度+密码+后填充‘F’到 16 字节）：
06123456FFFFFFFFFFFFFFFFFFFFFFFF

第二步，账号处理（账号去除校验位后 12 位+前填充‘0’到 16 字节）：
0000000000000000000001234567890 12

第三步，将第一步的结果与第二步结果异或，得到 PIN 块：
06123456FFFFFFFFFFFFEDCBA9876FED

第四步，SM4 加密第三步的 PIN 块得到 pinblock：
30D4AE4426EA5B0A9B4EF6D0274A0769

2 国际 RSA 方案说明

1、前端获取密码键盘生成非对称算法 RSA 公钥对主密钥进行公钥加密，将加密数据下发密码键盘;

2、密码键盘用非对称算法 RSA 私钥对主密钥密文进行解密获取主密钥明文;

6、前端用对称算法 DES 对工作密钥明文进行加密，将工作密钥密文下载密码键盘;

7、密码键盘进行 pinblock，采用工作密钥进行对称算法 DES 加密,返回密码密文;

8、前端进行密码密文解密;

注:

RSA 采用 1408 长度，指数为 65537

终端数据进行公钥加密前进行 PKCS#1 方式填充。格式如下说明，
其中的 BT 用 02，因为这里用到的是公钥加密。PS 为随机数。其中 D 为数据部分，D 数据可参照“D 数据解析说明”，其中 D 数据中包括密钥的明文（可随机产生的 16 进制密钥）

PKCS#1 附加模式

PKCS#1 标准定义了在用 RSA 公钥或私钥计算之前所使用的附加方式。在要加密或解密的数据之后附加的模式如下所示：

00 BT PS 00 D,

其中：

BT 为指示块类型的单个字节。

PS 为附加的字符串。

D 为数据。

附加块的所有长度等于 RSA 密钥模数的长度（字节形式）。

当用私钥时 BT 为 01；公钥时为 02。

3 测试数据

3.1 国密测试数据

SM2 公钥:
64C9095A3BE59937727130A2BD4787CEFDE29D823538A0AFD13D02F71CD68B77DDEA9D24753CF8E7A30B8D13AB7183A8945D639D33A966B198BD315D747AF3D7
SM2 私钥:
0F60EBDA337019D38B903C81D21BD3E4B69CC4AAB82972599F8173863E99A3A2
SM2 公钥加密主密钥密文:
A9753199C8D3A5E2F62194318C937077C3E1C3AA7E5A9D0358FFAE27D9DF16EA0B9914D2662412E40ADF95684E2731118255C7559DD27D50926A99ED0A5B032E07BF199DF03422CA6422191FBF91F8E07CEC3EAA4C5AA27F401355A5F4297FC138C730B474ABA7567301BB095DBE10CE
主密钥明文:
1FB99F2A1FFEFEEB6566BD985DA0113B
校验值:
02BA10B7B1C0F4E2
工作密钥密文:
85824EDB0A9D3032BC5DEE25D0EF2437
校验值:
AD07012B901E9B63
设备返回:
账号:123456789012
输入密码:123456
密文:1565B3ED128A399435F31E58DA2C7A4C

3.2 国际测试数据

RSA 公钥:
DBD41D66AE73DCC83F39268F674BC3B6E2DDEAD233DD51737A8BE31FBFA9058727CD3C8D6EE10EF1E14A9122C216A98377C0ECFF885F3FF67AC8FFDEA57CBEBCDA379557186E9DE179EA47BCBDF19A3F828A0AA80315417B9CC5F68A5CD78CECC2725CB2F0B7BDDB78322C23C2BBAEE10B58F543B34D14671BE75A1857151C6AA5525835F047E80B3E40EC9461760691FF12A94D7E961E1572F117CE287DDBDF1FF2E8EE8D443BCCC0BCEA2A6C5A9D99
RSA 私钥:
5563BA9BF52DDA580A7EF7A4829A6286BAEF3AD4B602C52DD72F59652EB

CC801ED0B02F7695790C7921CB5EDCB78A4160641718DFCFA0ACD827A6B
31A014A9BE90014148589C3745AB66BEC0E9035D48483BB8D1F488A02B5
C7B8C2102AB15A09AD97273CCF5604C23C00A1354D8B1E24E37F6E4FAAAF
782FEEF08A853CC4B2481FEAEBD26C09F166EDE5CDFA14BFC6B7FABE7961
398210C2A44EE52E5192366411C263E1337794C7806860372C8B7F5

RSA 公钥加密主密钥密文：

7626FA7215BC3FDEA7C80377E7F9245DCCC14E0E88D6673477A9DDFB0F08B5A744
6ADB89C41CC4DF5154A0F29A0C18E6A32939DB2EACB6FBA5073858C29556FD8CA
F42A2AA0C0AF6483ACF6D592228F0F81088F8C4BD50651A0CDD71FF8F7DA9551EF
FFD7856C22DBD7EC2A1FFF530CA972F25ACB651CC5E91DB8E688F4242056DF50FA
75AF62EA76CAFB0CF581A239533B6450279D891B28ADE7CC22E6C2521F4BC217B6
20FC4BE12178458C92F7F14

RSA 私钥解密数据：

00027D75BE7158D0B1012D01E78C4E71D2FE1E809C1831CE55330540DEE7124FC7
B51F2257AC679925CF20CD948956497FD91DFBCDF41C8127E73EEE84320737DCD0
105E15AF56DD9D5773C5C62A636774EF4CF751272F08CBF6167E2657098249D955
74A9FB35BD6ACD259E65C7453710EA18AA709B1CD0657641D76DAF16202F0D75A
116776ED8553B6492020B1421B28F20A6AA6E69D2E0F226717A441000CD865BBCA
D2A928C2C61B30E3BCB2A15

主密钥明文：

CD865BBCAD2A928C2C61B30E3BCB2A15

校验值：

3F7B196C9450227D

工作密钥密文：

85824EDB0A9D3032BC5DEE25D0EF2437

校验值：

8A76FC0AC86692D5

设备返回：

账号:123456789012

输入密码:123456

密文:9FAFBB85CB6E3536

4 新老加密方案交叉使用说明

新老加解密方案采用不同驱动接口 ，可以通过业务系统自由切换方案。保证可以回退。

密码键盘需要具有唯一序列号来实现密钥的一机一密。序列号规则：厂商标示+字符串(该字符串保证唯一，可以不规则编码)

密码键盘需要分区间地址存储新老密钥，保证兼容新老加密方案生产环境的交叉使用。

5　方案验证时间、地点

验证地点:

交通银行总行软件开发中心开发二部

验证时间:

2016/4/18-2016/4/22