金融 IC 卡根 CA 服务平台

常见问题手册（版本：2.0）

中国金融认证中心

2017 年 9 月 14 日

目录

1 基本流程

1.1 登录

金融 IC 卡根服务平台地址为：https://pboc.cfca.com.cn/rcaPlatform/。使用者通过 CFCA 申请安全员证书，下载安全员证书后即可登录。

初次使用此系统的安全员如果未注册机构，则显示如下注册界面：

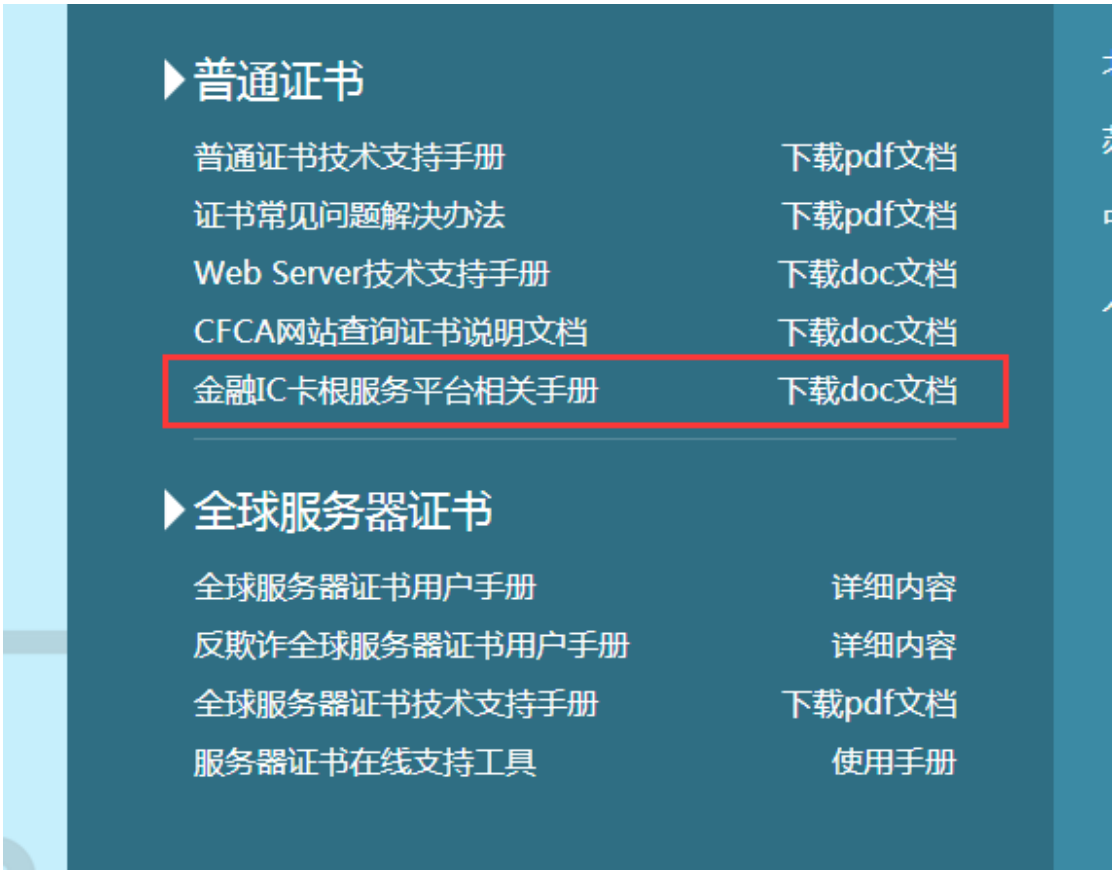
安全员填写注册信息后提交，等待管理员（银联）审核[1]后可继续操作。

1.2 证书公钥申请

点击发卡行申请书管理，选择录入发卡行申请书，显示录入发卡行申请书信息页面：

[1] 银联审核员联系方式：zhuchuan@unionpay.com；jnbai@unionpay.com

按照本行需求填写信息，提交后等待银联审核。审核通过后，流转到 CFCA 产生对应记录号。用户上传 INP 文件，再次等待 CFCA 签发 IC 卡公钥。详细手册请参考 PBOC 官网右上角的操作手册，或 CFCA 官网售后服务界面 http://www.cfca.com.cn/help/ 金融 IC 卡根服务平台相关手册。



2 常见问题

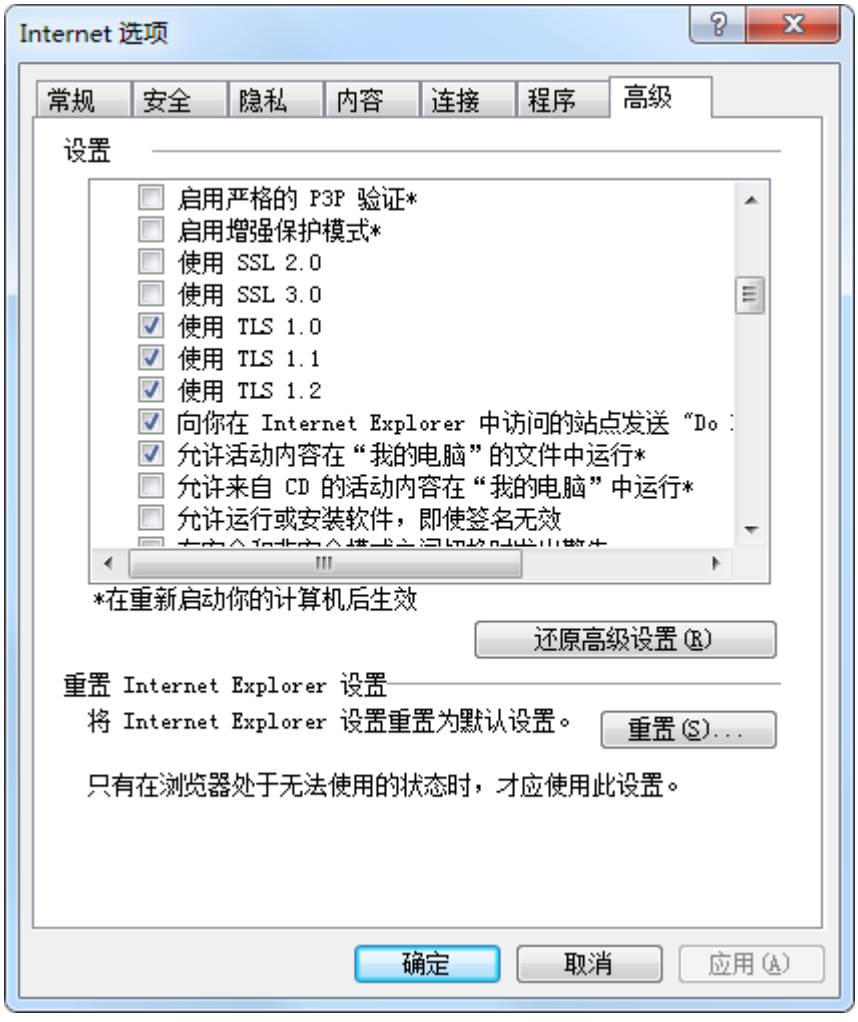
2.1 登录问题

2.1.1 没有弹出证书选择框，不能登录

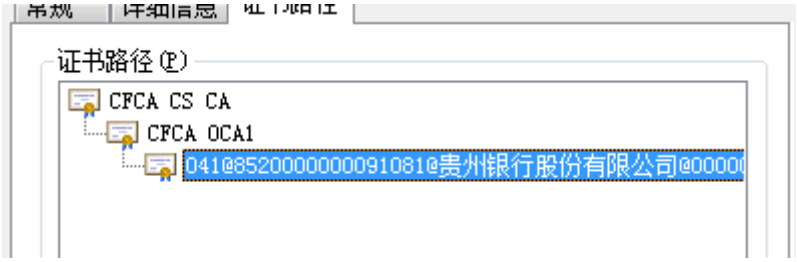
解决方法：

（1）确认登录网址，正确的登录地址为：https://pboc.cfca.com.cn/rcaPlatform/ 地址必须是 https 的，http 网址不能自动跳到正确的网址。

（2）调整 IE 设置，勾选 TLS1.0 或以上，其他不勾选，如下图所示。



（3）查看证书，确认证书带私钥及证书链并可用。正常的证书应该有三层，如下图所示：



如未有证书链，请登录 CFCA 官网进行下载，证书链下载地址：http://www.cfca.com.cn/file/cfca_vista.rar。

确认证书链正确安装后，通过体验平台进行验证证书是否可用。地址：https://cez.cfca.com.cn/cez/allCertApplication.client，首次登陆需要下载插件。

（4）证书验证通过，但是还是不能通过 IE 进行登录，可以通过 360 极速模式，或下载搜狗浏览器进行登录。可能原因为电脑 IE 有问题，证书文件不能正确读取。

（5）如证书验证不可选出安全员证书，请尝试是否能将安全员证书带私钥导出。如果不可以导出，怀疑系统是 GHOST 系统（一般因为缺少证书相关底层文件，此时证书已不能导出，如果没有证书文件，只能补发证书）。

2.1.2 选择证书后报错，错误码 9005

问题原因：

选择的证书不是金融 IC 卡的安全员证书，没有登录权限。

解决方法：

请先确定登录所选的证书是安全员证书，金融 IC 卡服务平台安全员的证书 DN 应为：041@XXXXX@银行名称@0000000X。如确认是 PBOC 的安全员证书，请联系 CFCA（400-880-9888）进行授权工作。

2.1.3 选择证书后报错，错误码 9006

问题原因：

选择的证书已经吊销，不可使用。

解决方法：

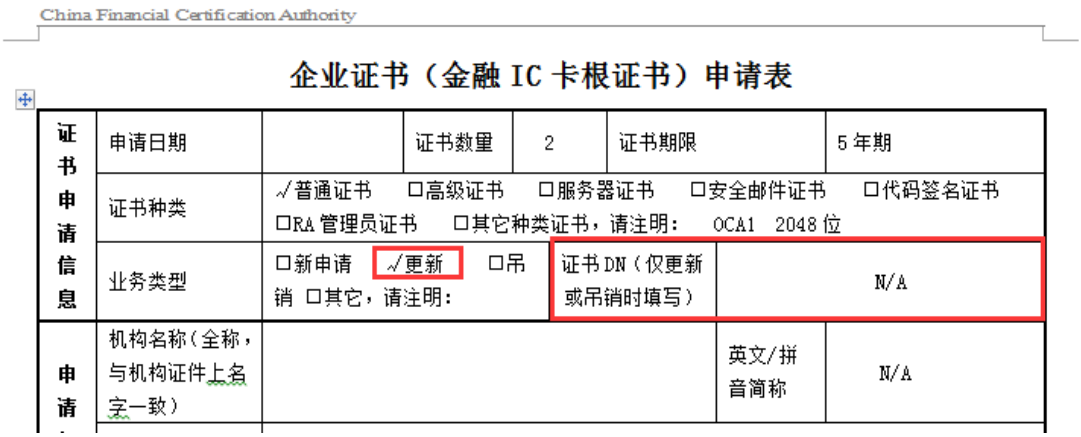
选择的安全员证书已吊销，请选择正确的安全员证书或进行安全员证

书换发操作。

2.2 安全员证书补发、换发流程

2.2.1 换发流程

金融 IC 卡平台安全员证书到期进行换发，需要填写《企业证书申请表-金融 IC 卡根证书.doc》。其中业务类型选择：更新，并需要填写之前安全员证书 DN，填写方法如下图所示。如果不知道以前安全员证书 DN，可联系 CFCA 在系统里查找相关记录。申请表其他内容按照表格要求填写即可，填写完成后将申请表发送给 pboc@cfca.com.cn。（pboc@cfca.com.cn 此邮箱只接受申请邮件，不解答任何问题，如有需要咨询的事宜，请联系 400-880-9888）。



China Financial Certification Authority

企业证书（金融 IC 卡根证书）申请表

证书申请信息	申请日期		证书数量	2	证书期限	5 年期
	证书种类	√普通证书 □高级证书 □服务器证书 □安全邮件证书 □代码签名证书 □RA 管理员证书 □其它种类证书，请注明： OCA1 2048 位				
	业务类型	□新申请 √更新 □吊销 □其它，请注明：		证书 DN（仅更新或吊销时填写）	N/A	
申请	机构名称（全称，与机构证件上名字一致）				英文/拼音简称	N/A

2.2.2 补发流程

安全员证书**未到有效期**，因各种原因遗失，需要进行证书**补发**。按照《企业证书申请表-金融 IC 卡根证书.doc》填写申请。其中业务类型选择“**其他**”**注明补发证书**，并填写需要补发的证书 DN，如不知道证书 DN，可联系 CFCA

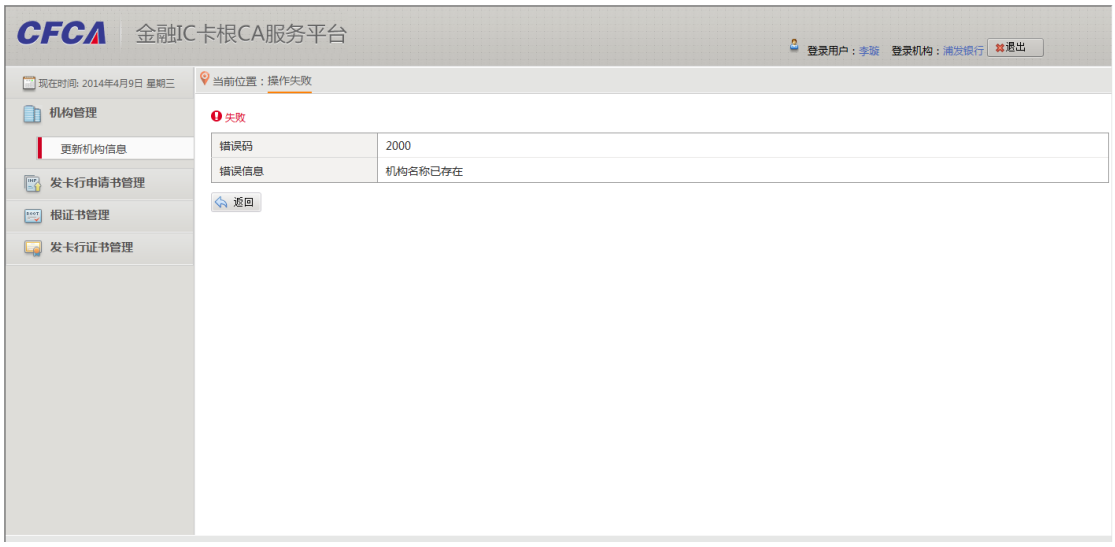
确认。客户需要将申请表发送给 pboc@cfca.com.cn，并在申请表中附上之前安全员证书申请的付款凭证。

企业证书（金融 IC 卡根证书）申请表

证书申请信息	申请日期		证书数量	2	证书期限	5 年期
	证书种类	√普通证书 □高级证书 □服务器证书 □安全邮件证书 □代码签名证书 □RA 管理员证书 □其它种类证书，请注明： OCA1 2048 位				
	业务类型	□新申请 □更新 □吊销 √其它，请注明：补发			证书 DN（仅更新或吊销时填写）	N/A

2.3 成员机构相关问题

2.3.1 机构名称已存在，错误码 2000



问题原因：

此机构信息在 PBOC 网站已存在，不可重复录入。

解决方法：

请确认机构名称输入是否正确。如果确认机构信息录入无误，但是依旧报错，请联系 CFCA 进行核实，联系电话 400-880-9888。

2.3.2 机构类型如何修改

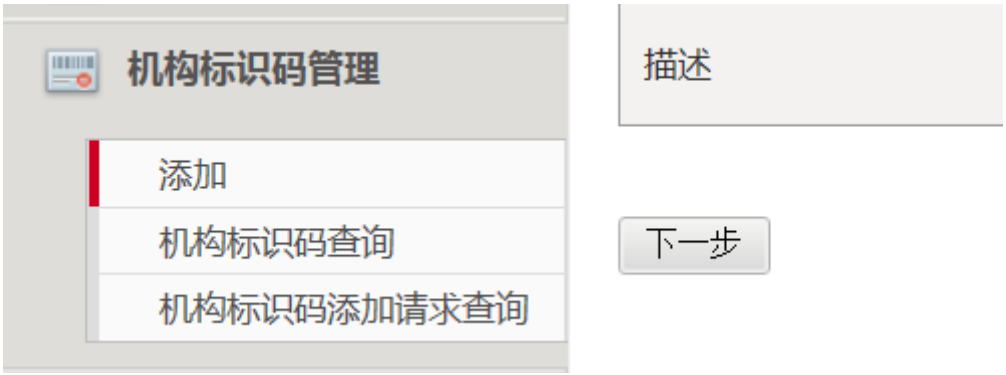
问题原因：

在注册机构信息时，选择机构类型选择错误。已经保存后想要更改。但是机构类型如下图所示不能选择更改。

解决方法：

机构类型如果选错了并且已经保存，则需要联系银联方申请更改。如银联方面同意更改，则由银联发邮件告知 CFCA，CFCA 在后台进行更改。

2.3.3 标识码更改



问题原因：

成员行从银联获得新的机构标识码，需要添加，如何处理？

解决方法：

登录平台点击“机构标识码查询”，查询机构标识码之后进入详情页，进行操作即可。系统会自动校验，校验通过即修改成功；校验失败则银联手动审核，无需 CFCA 后台修改。

2.3.4 BIN 号位数缺失

问题原因：

根据银联现有规则，证书管理中显示的是证书的信息，证书信息目前只能显示 8 位数字，所以此处的 BIN 号最多为 4 个字节，也就是 8 位数字。超过 8 位数字的，只能显示前 8 位，但是不影响使用。

而发卡行申请书管理中显示的是录入申请书时填写的，填写的多少位就是多少位。

如下图所示，最初的 BIN 号为 621623001，但是最后查看的 BIN 号为 62162300。

解决方法：

目前不影响使用，后续银联会出台新的规则。

2.4 申请金融 IC 卡公钥问题

2.4.1 不可申请生产类型发卡行证书

问题原因：

根据发卡行申请书管理下的要求，录入相关信息，但是选择生产类型的公钥证书后，BIN 号自动消失，并且不能填写 BIN 号。

解决方法：

此机构没有发生产类型证书的权利。请确认已将人行的批复（“中国人民银行 XX 支行关于 XX 银行金融 IC 卡借（贷）记卡发卡技术标准符合性和系统安全性审核的批复”）提供给了银联审核员（zhuchuan@unionpay.com；jnbai@unionpay.com）。如确认提供，可以联系 CFCA 在系统内查询是否更改了机构信息。如果未提供，请将批复提供给银联审核后更改机构状态。

2.5 申请已提交，审核相关问题

2.5.1 提交申请后，一直在审核

问题原因：

申请信息提交后，显示需要银联审核。

解决方法：

银联方面审核间隔是，每天审核三次，请耐心等待。如超过一个工作日还未审核，请联系银联人员。

2.5.2 审核通过，记录号为空

问题原因：

申请信息通过银联审核后，记录号未产生。

解决方法：

此记录号由 CFCA 产生，银联审核通过后大概一个工作日产生，请耐心等待。如长时间未产生，可以联系 CFCA 处理。

2.5.3 审核未通过

机构标识码	15454312	机构名称	丰城顺银村镇银行
机构类型	发卡机构	BIN号	621828661
记录号	请将记录号填写完整	发卡机构公钥类型	RSA
发卡机构公钥长度	1408	请求签发证书的根CA公钥索引	3 服务标识:01010000
申请日期	2014-10-21	申请原因	首次申请
发卡机构公钥证书申请类别	生产型公钥证书	证书失效时间	2021-12-31
卡BIN的审批通过时间	2014-09-25		
卡BIN发卡类型	借记卡	证书状态	审核未通过
描述	卡BIN有误		
证明文件	未上传证明文件		

问题原因：

申请公钥相关信息不准确，被银联退回。

解决方法：

未通过审核的原因，会在页面进行显示。因为此步骤是银联进行审核，如果客户有异议，需要联系银联审核员进行沟通。

2.5.4 录入发卡行申请书后被审核拒绝（索引错）

问题原因：

申请的均是索引为 9，1408 位证书。由银联方面审核退回，此退回原因是银联后台抛出。

机构标识码	15537552	机构名称	丽江永胜长江村镇银行股份有限公司
机构类型	发卡机构	BIN号	621676016
记录号		发卡机构公钥类型	RSA
发卡机构公钥长度	1408	请求签发证书的根CA公钥索引	9 服务标识:01010000
申请日期	2015-04-07	申请原因	首次申请
发卡机构公钥证书申请类别	测试型公钥证书	证书失效时间	2030-12-31
卡BIN的审批通过时间	2015-02-28		
卡BIN发卡类型	借记卡	证书状态	审核未通过
描述	索引错，应为0b，请阅读相关材料		

机构标识码	15147042	机构名称	仁怀蒙银村镇银行股份有限公司
机构类型	发卡机构	BIN号	62354331
记录号		发卡机构公钥类型	RSA
发卡机构公钥长度	1408	请求签发证书的根CA公钥索引	9 服务标识:01010000
申请日期	2015-04-09	申请原因	首次申请
发卡机构公钥证书申请类别	测试型公钥证书	证书失效时间	2030-12-31
卡BIN的审批通过时间	2015-04-09		
卡BIN发卡类型	借记卡	证书状态	审核未通过
描述	根CA公钥索引有误		

解决方法：

因现在无法发出 10 年有效期的 1408 证书，而一般情况下借记卡有效期默认是 10 年（只有选择借记卡才有此提示，选择信用卡就不会，因为信用卡有效期一般是 5 年），所以银联发出这样一个类似友情提示，如果用户

坚持申请 10 年内的 1408 位申请书，则联系银联，银联手动审核通过即可。

2.6 用户上传的 INP 文件时报错

2.6.1 错误码 3400

问题描述：

在发卡行申请证书管理，做发卡行申请书录入，在上传 inp 文件时，报错“导入发卡行公钥输入文件失败，错误码：3400”

解决办法：

（1）INP 文件中的密钥不能以 00 字节或者 FF 字节开头，INP 文件中的签名验证不过也不可以。如果不确认上传 INP 文件的信息，联系 CFCA 进行查看。

（2）INP 文件名字不能超过 12 个字符，但是对应名字命名序列号没有要求。比如生产的 INP 文件为 YL000187.INP，改成 YL000189.INP 也能上传成功。一般情况下不建议更改文件序列号。

2.6.2 错误码 3401

问题描述：

在发卡行申请证书管理，做发卡行申请书录入，在上传 inp 文件时，报错“发卡机构公钥证书申请文件中的公钥验证数字签名未通过，错误码：3401”。客户经过本行验证无问题，经过 CFCA 的 INP 文件查看工具验证，错误依旧是 3401，无详细内容。

解决办法：

根据银联对公钥证书签名要求，必须满足以下计算条件的数字签名才可以通过。告知客户依照以下要求，更改签名。

对任意长度的数据组成的报文 MSG 计算签名 S 的过程如下：

a) 计算 ZA=SM3[ENTLA || IDA || a || b || xG ||yG || xA || yA]。其中 IDA 固定设置为 16 字节定长的十六进制数据 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38；ENTLA 值为两个字节数据 0x00, 0x80；

b) 计算报文 MSG 的 32 字节的 HASH 值 h:= SM3 [ZA||MSG]；

c) 计算 Sign(SK)[h]，得到两个数字 r 和 s；

d) 数字签名 S 被定义为 S:= r||s，即数字签名 S 由数字 r 和 s 串联而成。

2.6.3 错误码 3402

问题原因：

发卡行公钥输入文件中服务标识与申请信息中不一致，导致上传 INP 文件后报错。

解决方法：

目前 CFCA 金融 IC 卡根服务平台，所有的根都是借贷记的，对应的服务标识如下：

借贷记：01010000
借　　记：01010100
贷　　记：01010200
准贷记：01010300

所以产生的 INP 文件中的服务标识只能是 01010000，如果 INP 文件中

的服务标识不是 01010000，则报错。解决此问题，请重新产生 INP 文件。

2.6.4 错误码 3404

问题原因：

上传的 INP 文件中的证书失效日期与系统中记录的不符。

解决方法：

如果 INP 文件中信息与证书申请信息不符，请重新生产 INP 文件并确保与系统中的一致，形成新文件后再重新上传尝试。

2.7 其他问题

2.7.1 截止 2016 年 7 月 11 日生产根 CA 证书信息

如下是截止到 2017 年 9 月 12 日金融 IC 卡根服务平台可以查询到的全部根 CA 证书的信息：

根CA系统名称	根CA密钥索引	算法	公钥模长	证书有效期
测试C0B(RSA1984)	0b	RSA	1984	2030-12-31
测试C0A(RSA1024)	0a	RSA	1024	2030-12-31
测试C09(RSA1408)	9	RSA	1408	2030-12-31
测试C08(RSA1152)	8	RSA	1152	2030-12-31
PBOC3.0生产C11(SM2)	11	SM2	256	2027-12-31
生产C04(RSA1984)	4	RSA	1984	2027-12-31
生产C03(RSA1408)	3	RSA	1408	2024-12-31
生产C02(RSA1152)	2	RSA	1152	2021-12-31
生产C01(RSA1024)	1	RSA	1024	2010-12-31
PBOC3.0测试C18(SM2)	18	SM2	256	2030-12-31

2.7.2 发卡行 CA 证书，无法在银行的系统中使用，报错公钥余项为空

问题原因：

此问题通常都是客户申请在 1984 的根下签发的 1408 的发卡行 CA 证书在使用中遇到的问题；

问题的根本原因是客户自己的发卡行 CA 系统没有严格遵循 PBOC 的规范，所以对根 CA 和发卡行 CA 密钥长度差导致公钥余项为空的现象无法进行处理。按照 PBOC 的规范，发卡行 CA 证书即使公钥余项为空，依然是应该可以可以正常使用的。

解决方法：

问题的解决办法只能是客户找发卡行 CA 的技术人员进行修改，确保可以正常使用公钥余项为空的发卡行 CA 证书。

2.7.3 申请不了公钥索引为 2 的公钥

问题原因：

选择了 1152 长度的公钥，并提交了申请，为什么审核不通过？

解决方法：

根据银联最新通知，自 2015 年 11 月 6 日起停止签发 1152 位发卡行证书。目前 1152 位发卡行证书有效期到 2021 年 12 月 31 日，已经申请并使用的可以继续使用，不再受理新的申请（1152 位的申请运行部会拒绝）。根据 IC 卡服务平台发出的公告《关于 2016 年度中国银联金融 IC 卡根 CA 公钥有效期更新的公告（网站）.docx》。如果有用户来电咨询，可告知用户不要申请 1152 位证书。

2.7.4 不能申请 1984 的发卡行 CA 证书

问题现象：

选择公钥长度为 1984，审核不通过。

解决方法：

根据公告《关于向 CFCA 申请 1984 位发卡行公钥证书的相关业务提示.pdf》，银联不再签发公钥长度是 1984 的公钥证书。发卡行 CA 公钥长度必须小于等于 1408，所以客户如申请 1984 位的发卡行公钥证书，将审核不通过。

2.7.5 PBOC3.0 发卡环境注意事项

3.0 发卡环境，一个 BIN 号，必须在申请国际算法（2.0）的发卡行证书的基础上选择申请国密算法（3.0）的发卡行证书，具备 3.0 环境的发卡机构，存在两种发卡情况：单算法（仅国际算法）和双算法（一个国际+一个国密）；也就是说，在现有受理环境下，国际算法的发卡证书是基础，国密算法的发卡行证书是可选项。