

附件

# 中金金融认证中心有限公司 数字证书设备认证测试流程

## 第一章 总则

**第一条** 为加强和规范中金金融认证中心有限公司（以下简称 CFCA）数字证书设备认证测试，依据《中金金融认证中心有限公司数字证书设备认证测试业务管理办法》（中金发〔2023〕5 号），制定本流程。

**第二条** 本流程适用于 CFCA 测试中心开展数字证书设备认证测试业务（以下简称认证测试），认证测试包括兼容性测试、预植联调测试和移动端测试。

**第三条** 本流程公布范围为 CFCA 和需要进行认证测试的外部厂商。

## 第二章 认证测试约束

**第四条** 兼容性测试可独立开展，移动端测试为可选测试项，预植联调测试需配合兼容性测试一起开展。

**第五条** SM2 算法为必选，RSA1024 算法需配合 RSA2048 等安全级别更高的 RSA 算法一起选择。

**第六条** 认证测试费用为包含三轮测试机会的费用，若测试机会用完仍未测试通过且需要继续测试时，厂商需要提交追加测试申请。

**第七条** 第一次提交预植联调测试的厂商除认证测试费用外，还需缴纳预植生产工具购置和维护费。收费详情见《中金金融认证中心有限公司数字证书设备认证测试收费标准》（以下简称收费标准）。

**第八条** 预植联调测试在有限次数内没有出现问题，并不代表被测设备的软硬件没有问题，被测设备软硬件的健壮性和稳定性需要厂商保障，不在本认证测试范围内。

**第九条** 不同封装形式的设备，需分别进行认证测试。

**第十条** 相同封装形式但内置程序不同的设备，需分别进行认证测试。

**第十一条** 认证测试期间若更换硬件设备或者重写设备COS，均需重新提交认证测试申请。

**第十二条** 认证证书有效期为三年。

### **第三章 认证测试流程**

**第十三条** CFCA 测试中心部门领导分配测试任务，指派 2 人或多人组成测试小组，明确测试小组成员中负责认证测试的 CFCA 联系人（以下简称 CFCA 联系人）和执行测试任务的测试人员。

**第十四条** 厂商资质审核

（一）厂商需提交给 CFCA 联系人如下相关资料

1. 厂商公司营业执照复印件加盖公章。
2. 设备说明书（内容应包含设备的正、反、侧面图片，说明设备安装 CFCA 数字证书的途径和使用场景等）。

(二) 测试小组对厂商提交的资料进行审核并进行整体评估，由 CFCA 联系人通过邮件反馈审核结果。审核需在五个工作日内完成。

### **第十五条 申请认证测试**

(一) 厂商联络人收到资质审核通过的通知后，需填写附件 1《中金金融认证中心有限公司数字证书设备认证测试申请表》（以下简称测试申请表）。

(二) 厂商可根据第十九条中描述的时间节点决定是否选择加急测试（加急测试即每轮测试不需要排队等待）。

(三) 若厂商对其设备的兼容性测试，除第二十四条中列出的平台外，还有其他平台需求（比如 MAC 平台、信创平台等），在测试申请表中选择追加测试并在“备注”一栏添加详细说明。

(四) CFCA 联系人指导厂商完成测试申请表的填写，依据收费标准告知厂商收费金额，厂商需将填写完成的测试申请表盖章后邮寄给 CFCA 联系人。

### **第十六条 缴费**

(一) CFCA 联系人通过邮件将 CFCA 的收款账号告知厂商。

(二) 厂商汇款成功后需向 CFCA 联系人提供汇款回执单和开发票信息，并预约开具发票。

### **第十七条 获取支持**

(一) 厂商可以从 CFCA 官网下载第二十四条和第二十五条中提到的 CFCA 相关接口调用规范，依据接口调用规范开发设备测试程序。

(二) 厂商可以通过 CFCA 邮箱 (support@cfca.com.cn) 获取数字证书的两码，通过 CFCA 的统一下载平台 (<https://cstest.cfca.com.cn>)，使用数字证书两码下载证书，以便做相应开发和内部测试工作。

### **第十八条 软硬件和相关资料提交**

(一) 厂商需将如下资料加盖公章邮寄给 CFCA 联系人

1. 国内产品提供国家密码管理局颁发的商用密码产品认证证书复印件，国外产品提供相应认证机构的证明复印件。

2. 如设备硬件命名与国密备案型号不同，需单独提供设备名称与国密备案型号的对应说明（无固定格式，按厂商行文格式即可）。

3. 设备是否符合国际标准 FIPS 140-2 的声明（无固定格式，按厂商内部行文格式即可）。

(二) 设备的电子版资料和程序均须由厂商联络人以邮件形式提交给 CFCA 联系人。

(三) 提供硬件设备时，需将 CFCA 联系人提供的长度为 16 位的数字证书 ID 打在设备的外壳及芯片内。提供 4 台设备用于兼容性测试，每种算法提供 16 台设备用于预植联调测试。

(四) 厂商需提交的设备测试程序包括管理工具、预植动态库、端口绑定工具以及初始化工具等辅助程序。其中预植动态库需兼容所有在认证证书有效期内的设备（因预植环境不兼容导致动态库无法兼容的情况除外），端口绑定工具需在桌面创建快捷方式且名称需包含能识别厂商的文字。

(五) 移动端测试需提交移动端可安装的 Demo 程序，功能包含验证 PIN 码、读取证书、P7 分离式交易报文签名、P7 分离式非交易报文签名，签名原文支持修改和拷贝、签名结果支持拷贝。CFCA 测试人员随机选用一台 Android 设备和一台 IOS 设备作为移动端测试机器。

(六) 厂商提供的设备测试程序及辅助程序，应遵循高效无冲突原则，若程序操作复杂、相互冲突等原因影响效率，厂商需根据测试人员的建议对程序进行优化。

(七) 厂商需提供所提交程序对应的使用说明书，若测试设备为液晶型二代 USB Key，还需提供特定交易报文。

(八) 认证测试过程中，厂商若更改设备测试程序，再次提交测试时需升级程序的版本号。

## 第十九条 预约测试

(一) 厂商通过邮件方式与 CFCA 联系人预约测试时间。

(二) 兼容性测试和移动端测试的每轮测试时间为三个工作日，预植联调测试的每轮调试时间为四个小时。测试采用每轮预约排队机制，排队顺序按预约先后排列，每轮最长排队周期为 15 个工作日。

(三) 若厂商不确定预植动态库是否兼容之前认证通过的设备, 可在本次提交的设备测试通过后, 与 CFCA 联系人预约测试环境, 由厂商自行验证。

## **第二十条 测试与反馈**

(一) 兼容性测试和移动端测试由 CFCA 测试人员独立完成, 预植联调测试厂商可选择由 CFCA 测试人员独立完成还是厂商人员来 CFCA 现场测试。

(二) CFCA 测试人员依据第二十四条和第二十五条编写测试用例, 测试小组评审通过测试用例后方可开展测试工作。

(三) 测试人员记录每轮的测试结果并编写问题单, 问题单经测试小组评审后, 由 CFCA 联系人以邮件形式反馈给厂商并说明剩余轮次。若三轮测试机会用完仍未测试通过, 需在测试申请表中勾选追加测试并依据收费标准完成加测费用缴纳后, 方可继续进行测试。

## **第二十一条 解答与调试**

(一) 厂商收到问题反馈后, 可与 CFCA 联系人沟通了解测试问题。

(二) 若厂商无法重现兼容性测试的问题, 可与 CFCA 联系人预约现场或远程调试, 在测试申请表中勾选追加测试并依据收费标准缴纳调试费用。

## **第二十二条 认证测试通过及归档**

(一) 设备通过认证测试后, 由测试人员将设备和厂商提交的相关纸质资料归档, 并编写测试报告提交至测试小组评

审，评审通过后由 CFCA 联系人将设备程序和测试报告归档到测试中心指定服务器路径并邮件告知负责设备预植生产的部门联系人。

（二）测试人员根据附件 2《认证证书模板》制作认证证书并提交至测试小组评审，评审通过后由 CFCA 联系人打印认证证书并提交盖章申请，CFCA 联系人将盖章后的纸质证书邮寄给厂商。

（三）CFCA 联系人将测试通过的相关程序版本号添加到测试申请表并提交盖章申请，CFCA 联系人将盖章后的测试申请表邮寄给厂商。

（四）测试人员根据附件 3《官网公布的材料模板》编写官网公布的材料并提交至测试小组评审，评审通过后由 CFCA 联系人定期以邮件形式发送至网站发布信息维护员邮箱并跟进发布进度。

（五）厂商收到认证证书后应仔细核对，内容如有不符，请于五个工作日内与 CFCA 联系人确认并更换。其他需要更换证书的情况，需依据收费标准完成缴费。

### **第二十三条 销毁方式**

（一）测试小组成员根据认证证书过期情况，以邮件形式向部门领导发起销毁申请，部门领导批准后，由测试小组中至少两人执行销毁并填写附件 4《数字证书设备销毁记录表》。

（二）采用碎纸机的方式对纸质资料销毁，采用损坏罩壳外观的方式对硬件设备进行销毁。

## 第二十四条 兼容性测试依据

(一) 设备兼容性测试是基于在行业内广泛应用的 CFCA 数字证书，并配合客户端专用的测试工具，进行设备兼容 CFCA 数字证书体系的测试。

(二) CFCA 的 RSA 证书体系及客户端专用的测试工具依据微软标准 CSP 接口、CFCA《RSA 数字证书申请及应用 CSP 接口调用规范》和 CFCA《RSA 数字证书申请及应用 PKCS11 接口调用规范》进行开发。

(三) CFCA 的 SM2 证书体系及客户端专用的测试工具依据 CFCA《SM2 数字证书申请及应用 CSP 接口调用规范》和 CFCA《SM2 数字证书申请及应用 PKCS11 接口调用规范》进行开发。

(四) 设备及其驱动程序需要支持的环境包括 Windows7 x86 IE 浏览器、Windows8 x86 IE 浏览器、Windows10 x64 Edge 浏览器、Windows11 x64 系统 Edge 浏览器。

### (五) 主要测试内容

1. 通过 CFCA 数字证书下载平台和证书两码，对设备执行 SM2 及 RSA 证书的下载测试。

2. 对设备中已下载的 CFCA SM2 证书和 RSA 证书，进行消息签名验签和文件签名验签测试（签名验签算法有 SHA1、SHA256、SHA384、SHA512、SM3）。

3. 对设备中已下载的 CFCA SM2 证书和 RSA 证书，进行消息加解密和文件加密解密测试（加解密算法有 RC4、3DES、现国密标准、原国密标准）。

4. 设备管理工具的常规功能测试。



5. 对设备中已下载的 CFCA SM2 证书和 RSA 证书及管理工具进行边缘化测试。

## 第二十五条 预植联调测试依据

(一) CFCA 的数字证书预植体系及客户端专用的测试工具依据 CFCA《预植证书 DN 规则》和 CFCA《预植数字证书接口调用规范说明》进行开发。

(二) 预植联调测试的操作系统同 CFCA 预植生产的操作系统为 Windows10 x64。若 CFCA 预植生产的操作系统发生变更，预植联调测试的操作系统需同步变化。

(三) 使用 CFCA 的预植生产工具对设备和预植动态库进行常规功能测试，使用 CFCA 预植检测工具，对设备和预植动态库进行边缘化测试。

(四) 设备的预植效率要求如下表所示：

|            | 单台设备(s) | 16 台设备(s) |
|------------|---------|-----------|
| RSA1024 单证 | ≤5      | ≤20       |
| RSA1024 双证 | ≤10     | ≤25       |
| RSA2048 单证 | ≤10     | ≤30       |
| RSA2048 双证 | ≤15     | ≤40       |
| SM2 单证     | ≤5      | ≤20       |
| SM2 双证     | ≤10     | ≤25       |
| 复合证书       | ≤15     | ≤40       |

(五) 相同算法类型的单台设备和 16 台设备，分别测试十次，在测试过程中无报错、无异常、效率达标且通过预植检测工具检测成功，则视为预植联调测试通过。

## 第四章 附则

**第二十六条** 本流程由测试中心负责修订和解释，自发布之日起实施。

- 附件：
1. CFCA 数字证书设备认证测试申请表
  2. 认证证书模板
  3. 官网公布材料模板
  4. 数字证书设备销毁记录表模板

## 版本控制信息

| 制度编号*            | 版本号* | 日期       | 主办部门 | 主办人 | 拟定（修订）说明                                  |
|------------------|------|----------|------|-----|---|
| CFCA-JSGL-L3-005 | 3.0  | 2023-2-6 | 测试中心 | 杨会淑 | 重新修订原《中金金融认证中心有限公司智能卡测试业务管理办法（修订版 2）》中的流程 |

附件 1

CFCA 数字证书设备认证测试申请表

|                  |          |   |   |
|------------------|----------|---|---|
| 申请日期             |          |   |   |
| 测试业务             |          | <input type="checkbox"/> 兼容性测试 <input type="checkbox"/> 预植联调测试 和 兼容性测试<br><input type="checkbox"/> 移动端测试 <input type="checkbox"/> 加急测试 <input type="checkbox"/> 追加测试  |   |
| 设备类型             |          | <input type="checkbox"/> 一代 Key <input type="checkbox"/> 二代 Key <input type="checkbox"/> 蓝牙 Key <input type="checkbox"/> 音频 Key<br><input type="checkbox"/> 其他终端设备  |   |
| 算法类型             |          | <input type="checkbox"/> SM2 <input type="checkbox"/> SM2 和 RSA2048 <input type="checkbox"/> SM2、RSA2048 和 RSA1024<br><input type="checkbox"/> 复合证书（RSA2048+SM2） <input type="checkbox"/> 复合证书（RSA1024+SM2） |   |
| 数字证书类型           |          | <input type="checkbox"/> 单证 <input type="checkbox"/> 双证    （此处可详细列出算法类型对应的数字证书类型）   |   |
| 测试收费方式           |          | 测试三轮，费用_____万元人民币（费用请咨询 CFCA 联系人）   |   |
| 测试目的             |          |   |   |
| 企<br>业<br>信<br>息 | 企业名称     |   |   |
|                  | 单位地址     | （此处填写公司的注册地址，CFCA 颁发的纸质证书中同步填写该地址）  |   |
|                  | 联系人      |   | （企业盖章）  |
|                  | 联系人电话    |   |   |
|                  | 企业领导（签名） |   |   |
| 设<br>备<br>信<br>息 | 硬件型号     | _____ 设备  |   |
|                  | 兼容性程序    | 管理程序名称： _____<br>版本号：（首次提交的版本号） 测试通过的版本号：（测试通过后填写）<br>安装程序名称： _____<br>版本号：（首次提交的版本号） 测试通过的版本号：（测试通过后填写）  |   |
|                  |          | 预植联调程序  | 端口绑定名称： _____<br>版本号：（首次提交的版本号） 测试通过的版本号：（测试通过后填写）<br>预植动态库名称： _____<br>版本号：（首次提交的版本号） 测试通过的版本号：（测试通过后填写） |
|                  | CSP 名称   |   |   |

|            |                 |   |           |
|------------|-----------------|---|-----------|
|            | 需求银行信息（没有则不需填写） | 需求银行名称：_____  |           |
|            |                 | 数字证书 ID 前六位：_____                                     |           |
|            | 预植动态库兼容情况       | 本次提交的动态库为通用版，兼容之前所有项目（如有特殊项目无法兼容，请列出）                 |           |
| CFCA<br>意见 | 是否同意测试          | <input type="checkbox"/> 是 <input type="checkbox"/> 否 | （CFCA 盖章） |
|            | CFCA 经办人        |   |           |
|            | CFCA 部门领导（签名）   |   |           |
| 备注         |                 |   |           |

注 1：本表一式两份，申请单位保留一份，CFCA 保留一份，CFCA 只负责本表信息的有效性；

注 2：申请单位必须遵守 CFCA 数字证书设备认证测试的政策和规定，按规定提供**公司资质证明复印件（加盖公章）、一套产品化的设备和相关文档**，供 CFCA 审查、存档。

附件 2

认证证书模板

(本模板可根据实际情况进行调整)

范本<1>



数字证书设备认证证书

(NO. CFCAXXXXXXXXXX)

兹证明:

此处填写公司名称

此处填写公司地址

此处放设备图片

此处填写设备型号 设备, 符合 CFCA 数字证书设备兼容性认证测试和数字证书设备预植认证测试的要求, 可以实现 CFCA 证书所要求硬件完成基于 USB 通道的密钥管理、证书管理、证书应用及预植生产功能。

CSP 名称:

安装程序名称和版本号:

预植动态库名称和版本号:

支持的证书类型和哈希算法: “√”代表支持; “X”表示不支持; “—”表示不涉及

| 测试场景<br><br>证书类型 | 测试项 |    | 哈希算法 |        |        |        |     |
|------------------|-----|----|------|--------|--------|--------|-----|
|                  | 兼容性 | 预植 | SHA1 | SHA256 | SHA384 | SHA512 | SM3 |
| RSA2048 单证       | √   | √  | √    | √      | √      | √      | —   |
| RSA2048 双证       | √   | √  | √    | √      | √      | √      | —   |
| SM2 单证           | √   | √  | —    | —      | —      | —      | √   |
| SM2 双证           | √   | √  | —    | —      | —      | —      | √   |

发证日期：  
有效期至：

中金金融认证中心有限公司  
(盖章处)

范本<2>



数字证书设备认证证书

(NO. CFCAXXXXXXXXXX)

兹证明：

此处填写公司名称

此处填写公司地址

此处放设备图片

此处填写设备型号设备，符合 CFCA 数字证书设备兼容性认证测试和数字证书设备预植认证测试的要求，可以实现 CFCA 证书所要求硬件完成基于 USB 通道的密钥管理、证书管理、证书应用和预植生产功能和基于蓝牙通道的证书应用功能。

CSP 名称：  
安装程序名称和版本号：  
预植动态库名称和版本号：

支持的证书类型和哈希算法：“√”代表支持；“X”表示不支持；“—”表示不涉及

| 测试场景<br>证书类型 | 测试项 |    | 哈希算法 |        |        |        |     |
|--------------|-----|----|------|--------|--------|--------|-----|
|              | 兼容性 | 预植 | SHA1 | SHA256 | SHA384 | SHA512 | SM3 |
| RSA1024 单证   | √   | √  | X    | √      | √      | √      | —   |
| RSA1024 双证   | √   | √  | X    | √      | √      | √      | —   |
| RSA2048 单证   | √   | √  | X    | √      | √      | √      | —   |

|                                 |   |   |   |   |   |   |   |
|---------------------------------|---|---|---|---|---|---|---|
| RSA2048 双证                      | √ | √ | X | √ | √ | √ | — |
| SM2 单证                          | √ | √ | — | — | — | — | √ |
| SM2 双证                          | √ | √ | — | — | — | — | √ |
| 复合证书<br>(RSA2048 单证<br>+SM2 双证) | √ | √ | √ | √ | √ | √ | √ |

备注:

1. 交易报文签名支持 SHA256、SHA384、SHA512 和 SM3 哈希算法。
2. 非交易报文签名支持 SHA1 和 SM3 哈希算法。

发证日期:

有效期至:

中金金融认证中心有限公司  
(盖章处)



附件 3

官网公布材料模板

(本模板可根据实际情况进行调整)

| 设备外观 | 证书编号 | 厂商名称 | 型号 | 测试项 | 有效期 |
|------|------|------|----|-----|-----|
|      |      |      |    |     |     |

附件 4

数字证书设备销毁记录表模板

(本模板可根据实际情况进行调整)

| 认证证书<br>编号 | 认证证书<br>有效期 | 厂商名称 | 设备类型 | 设备数量 | 销毁日期 | 执行人员 |
|------------|-------------|------|------|------|------|------|
|            |             |      |      |      |      |      |