

**上海清算所  
独立生产系统客户端  
数字证书升级改造推广  
接入配置手册**

2022 年 7 月

## 1 总体要求

上海清算所独立生产系统包括利率互换集中清算（IRS）系统、信用违约互换清算（CDS）系统、航运及大宗衍生品清算（FFA）系统、标准化利率产品（BDF）系统、招标发行（BIS）系统、证书管理（CMS）系统，其中 IRS 系统、CDS 系统、FFA 系统、BDF 系统、CMS 系统通过浏览器客户端访问，BIS 系统通过桌面客户端访问。

根据数字证书改造推广安排，上述独立生产系统客户端拟切换至支持 SM 密码算法的客户端。接入前，必须先完成浏览器插件、UKEY 驱动、代理软件等相关软硬件的安装配置，并完成防火墙等网络策略的调整，同时满足操作系统、浏览器的版本要求。

各系统具体要求如下：

| 序号 | 系统名称   | 操作系统                       | 证书                     | UKEY      | 浏览器要求          | 其他软件要求                                                 | 防火墙开通要求                                         |
|----|--------|----------------------------|------------------------|-----------|----------------|--------------------------------------------------------|-------------------------------------------------|
| 1  | IRS 系统 | Windows7<br>或<br>Windows10 | CFCA 企业高级证书，通过证书管理系统申请 | CFCA UKEY | IE11           | 1. UKEY 驱动<br>2. 跨浏览器插件（NetSignCNG）<br>3. 代理软件（BiSafe） | 地址：191.168.1.131<br>加密链路端口：7202<br>非加密链路端口：7203 |
| 2  | CDS 系统 | Windows7<br>或<br>Windows10 | CFCA 企业高级证书，通过证书管理系统申请 | CFCA UKEY | Chrome（67 及以下） | 1. UKEY 驱动<br>2. 跨浏览器插件（NetSignCNG）<br>3. 代理软件（BiSafe） | 地址：191.168.1.155<br>加密链路端口：7212<br>非加密链路端口：7222 |
| 3  | BDF 系统 | Windows7<br>或<br>Windows10 | CFCA 企业高级证书，通过证书       | CFCA UKEY | IE11           | 1. UKEY 驱动<br>2. 跨浏览器插件（NetSignCNG）<br>3. 代理软件         | 地址：191.168.1.150<br>端口：7855（会员）                 |

|   |        |                            |                                                    |              |                        |                                                                   |                                                    |
|---|--------|----------------------------|----------------------------------------------------|--------------|------------------------|-------------------------------------------------------------------|----------------------------------------------------|
|   |        |                            | 管 理 系<br>统 申 请                                     |              |                        | (BiSafe)                                                          | 、7844（代理客<br>户）                                    |
| 4 | FFA 系统 | Windows7<br>或<br>Windows10 | CFCA 企<br>业 高 级<br>证书，通<br>过 证 书<br>管 理 系<br>统 申 请 | CFCA<br>UKEY | IE11                   | 1. UKEY 驱动<br>2. 跨浏览器插件<br>（NetSignCNG）<br>3. 代 理 软 件<br>（BiSafe） | 地址：191.168.<br>1.135<br>端口：6666（清<br>算会员、经纪公<br>司） |
| 5 | BIS 系统 | Windows7<br>或<br>Windows10 | CFCA 企<br>业 高 级<br>证书，通<br>过 证 书<br>管 理 系<br>统 申 请 | CFCA<br>UKEY | -                      | 1. UKEY 驱动<br>2. 招标发行系统<br>承销商客户端<br>3. 代理软件（BiS<br>afe）          | 目 的 地 址：<br>191.168.1.137<br>端口：6556（承<br>销商）、6555 |
| 6 | CMS 系统 | Windows7<br>或<br>Windows10 | CFCA 企<br>业 高 级<br>证书，通<br>过 证 书<br>管 理 系<br>统 申 请 | CFCA<br>UKEY | Chrome<br>(84 及<br>以下) | 1. UKEY 驱动<br>2. 跨浏览器插件<br>（NetSignCNG）<br>3. 代 理 软 件<br>（BiSafe） | 目 的 地 址：<br>191.168.1.170<br>端口：<br>8180           |

## 2 UKey 准备

可根据市场机构需要,进行证书申请时自行选择“新发 UKEY”（由 CFCA 制证）或 “不需 UKEY”（由会员机构制证）。

### 2.1 选择 “新发 UKey”（由 CFCA 制证）

#### 2.1.1 安装 UKey 驱动程序

会员机构收到 CFCA 制证及快递的 UKey 后，插入 UKey 到电脑端，双击 UKey 驱动的盘符图标或打开 UKey 盘符后双击 UyeeServiceInstall.Enterprise.exe 安装程序，按向导提示点击下一步即可完成安装。

因 CFCA 的 UKey 批次存在差异，驱动程序安装文件及界面风格可能与下文中的说明或图片存在差异，具体以实际获取的为准。

#### 2.1.2 修改 PIN 码

UKey 在第一次使用时需修改 PIN 码，插入 UKey 等系统提示检测到新设备后，在右下角任务栏图标 ，即可显示 UKey 内容。



点击修改 PIN 码后，按提示输入当前 PIN 码和符合要求的新 PIN 码（最短 8 位，最长 16 位，必须含有数字、字母、符号中两种或两种以上组合，字母区分大小写），再点击确定保存。第一次修改时当前 PIN 码为 UKey 的初始 PIN 码：“Cfca123!”。

The screenshot shows a modal dialog box titled '修改PIN码' (Change PIN). It contains three input fields: '当前PIN码' (Current PIN), '新PIN码 \*' (New PIN), and '确认PIN码 \*' (Confirm PIN). Below the input fields, there is a note: '\* 新PIN码必须为数字、字母、符号中的两种或两种以上类型组合。PIN码长度限制为 8 到 16 位' (The new PIN must be a combination of two or more types of digits, letters, and symbols. The PIN length is limited to 8 to 16 digits). At the bottom of the dialog, there are two buttons: '确定' (Confirm) and '取消' (Cancel). The dialog is centered on the screen and has a white background with a thin border.

## 2.2 选择“不需 UKEY”（由会员机构制证）

会员机构需要自己制证时，经办人将收到“CFCA 企业证书两码”邮件，点击“一键制证链接”，打开 CFCA 制证服务平台页面（请使用 Windows 操作系统+Chrome 浏览器 60 以上版本操作），在“订单详情”页中进行制证操作。插入待制证 Ukey，点击“自

制证”，在弹框中点击“获取 UKey 序列号”后进行一键制证，输入 UKey 密码，验证通过后制证完成。

CFCA | 制证服务平台

订单详情

客户自制证

UKeyId: 218K000023 [获取Ukey序列号](#)

请检查UKeyId与硬件Ukey外壳上标注的序列号是否相同。

取消

一键制证

|       |                       |           |  |
|-------|-----------------------|-----------|--|
| 订单ID  | OI_220708101216098334 | 流水号       |  |
| 经办人电话 | 00000450              | 经办人邮箱     |  |
| 订单类型  | 证书新发                  | 订单状态      |  |
| 机构名称  | 97072580              | 收费金额      |  |
| 付款状态  | 无需付款                  | ukey序列    |  |
| 开票状态  |                       | 补发订单原订单ID |  |
| 快递公司  |                       | 运单号       |  |

付款

解绑

印制证

申请开票

制证控件下载

向晓天

单时间: 2022-07-08 10:12:16

序列号: 1050478056

费用细节: 企业证书费用: 100元/张 (1年);

锁状态: 无需解锁

快速状态

收货信息

联系客服

客户自制证

UKeyId: 218K000023 [获取ukey序列号](#)

请检查U **CFCA 中国金融认证中心 | Uyee 优易** 是否相同。

请输入PIN码

一键制证

确定

取消

收费金额 100

### 3 跨浏览器插件安装（IRS、CDS、FFA、BDF）

#### 3.1 安装插件程序

在操作终端 PC 机上双击 NetSignCNG v2.1.141.2.exe 驱动安装程序，使用管理员权限按向导提示点击下一步即可完成安装。安装完成后建议重启终端操作系统。

#### 3.2 安装后验证

运行 services.msc,打开服务管理界面，确保 NetSignCNGGuard Services 已启动，如下图所示。

|                                     |          |        |      |
|-------------------------------------|----------|--------|------|
| Net.Tcp Port Sharing Service        | Prov...  | 禁用     | 本地服务 |
| Netlogon                            | 为用...    | 手动     | 本地系统 |
| NetSignCNGGuardService              | infos... | 已启动 自动 | 本地系统 |
| Network Access Protection Agent     | 网络...    | 手动     | 网络服务 |
| Network Connections                 | 管理...    | 已启动 手动 | 本地系统 |
| Network List Service                | 识别...    | 已启动 手动 | 本地服务 |
| Network Location Awareness          | 收集...    | 已启动 自动 | 网络服务 |
| Network Store Interface Service     | 此服...    | 已启动 自动 | 本地服务 |
| Office 64 Source Engine             | 保存...    | 手动     | 本地系统 |
| Office Software Protection Platform | Ena...   | 已启动 手动 | 网络服务 |
| Offline Files                       | 脱机...    | 已启动 自动 | 本地系统 |

## 4 加密链路配置

独立生产系统客户端接入默认使用加密链路，可通过硬件网关和代理软件两种方式接入，各市场机构可根据实际情况选用其中一种方式。

### 4.1 网关配置接入（方式一）

市场机构需事先自行采购经国家密码局认证、符合 GMT0025 和 GMT0028 技术标准的密码通信设备，并在设备提供商支持下完成网络配置，各系统连接的具体服务地址端口见总体要求部分。

密码通信设备上必须在全局 CA 证书列表中，安装以下指定的根证书作为信任域：

CFCA\_CS\_SM2\_CA.cer

CFCA\_SM2\_OCA1.cer

CFCA\_SM2\_OCA31.cer

CFCA\_ACS\_SM2\_CA.cer

根证书文件可从 CFCA 网站上下载：



设备的相关通信配置中，SSL 密码套件要求仅配置 SM 相关算法套件，具体如下：

ECC-SM4-SM3

ECDHE-SM4-SM3

网关配置的后台服务地址见后附表。

## 4.2 终端代理软件（方式二）

注意：Bisafe 代理软件包中将提供预先配置的各业务系统地址，市场机构可根据实际情况进行修改。

### 1. 软件安装

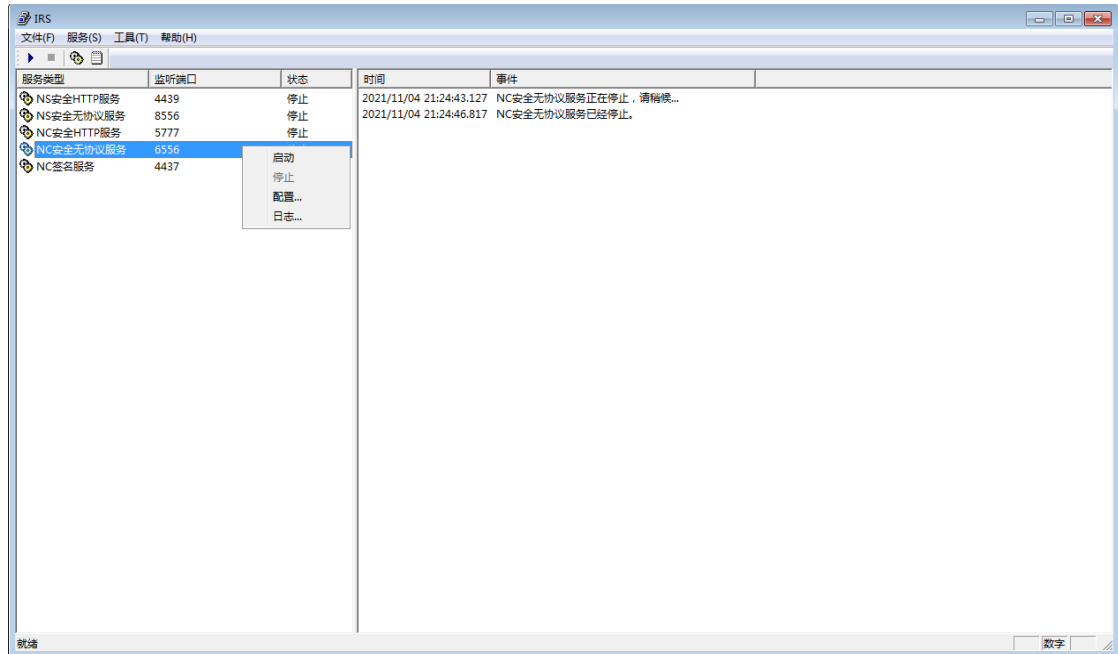
(1) 创建 BiSafe 3.18 的安装目录，建议该目录创建在 C 盘根目录下或者 C:\Program Files(x86) 目录下。

(2) 解压 BiSafe318.zip 至安装目录。

(3) 将 BiSafe.exe 快捷方式发送至桌面。

## 2. 软件配置

(1) 双击桌面快捷方式，打开 BiSafe 软件，选择 NC 安全无协议服务，右键点击配置



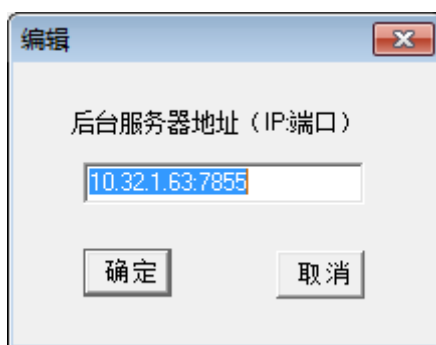
(2) 在配置对话框中，选择“Server 配置”页，点击编辑



(3) 在“监听的 IP 端口号”中填入本地监听的 TCP 端口号，不与部署该软件终端的其他 TCP 端口冲突即可。建议与需要连接业务系统网关服务端口保持一致，详见总体要求部分。



(4) 点击“编辑”按钮，填入后台服务器地址和端口（即 SSL 网关服务地址），格式为“服务地址:服务端口”。截图仅为示例，不代表真实生产地址或端口。



(5) 选择“SSL 配置”页



使用方式选择“使用硬方式”

以对于 CFCA 的优易品牌 UKEY 为例，安全模块库位置为：

C:\Windows\SysWOW64\UyeeSKF.shclearing.dll

令牌名称默认填：ShangHaiClearingHouse

(6) 选择“CRL 和 CA”页



选中并点击“删除”按钮，将 CA 配置列表项全部删除。

再点击“添加”按钮添加生产环境根证书（建议放在非中文路径下），其中证书文件名选择“CFCA\_SM2\_OCA1.pem”，不按发布点发布



(7) 选择“高级配置”页

等待超时（秒数）：建议配置为 3000

(8) 点击“确定”按钮完成配置

(9) 手工修改配置文件

用文本编辑器打开配置文件，路径为：BiSafe 安装目录  
\ncnops\config.ini。

将配置文件 [Cr1] 选项区域中的选项 enable=1 改为  
enable=0，并保存。

### 3. 启动代理服务

(1) 插入 UKEY，确保 UKEY 被终端识别。

(2) 选择配置好且处于停止状态的 NC 无协议安全服务，右键  
点击启动，并输入 UKEY 的 PIN 码。

(3) 右侧日志栏显示“NC 安全无协议服务已启动”，说明服务  
启动成功。

### 4. 停止代理服务

(1) 选择已启动的 NC 无协议安全服务，右键点击“停止”。

(2) 右侧日志栏显示“NC 安全无协议服务已停止”，说明服务  
停止成功。

附表：各业务系统配置生产服务地址

| 序号 | 系统名称   | 配置地址                                               |
|----|--------|----------------------------------------------------|
| 1  | IRS 系统 | 191.168.1.131:7202                                 |
| 2  | CDS 系统 | 191.168.1.155:7212                                 |
| 3  | BDF 系统 | 191.168.1.150:7855（会员）<br>191.168.1.150:7844（代理客户） |
| 4  | FFA 系统 | 191.168.1.135:6666                                 |
| 5  | BIS 系统 | 191.168.1.137:6556                                 |
| 6  | CMS 系统 | 191.168.1.170:8180                                 |

## 5 客户端启动登录

在代理软件服务启动状态下，根据所配置服务的本地监听端口号及业务系统访问 URL 访问客户端。

**例如：**本地配置的监听端口号为 6556，访问 CDS 系统。

原客户端访问方式为

<http://10.33.21.31:7002/client>

数字证书改造推广后客户端访问方式为

<http://127.0.0.1:6556/client>

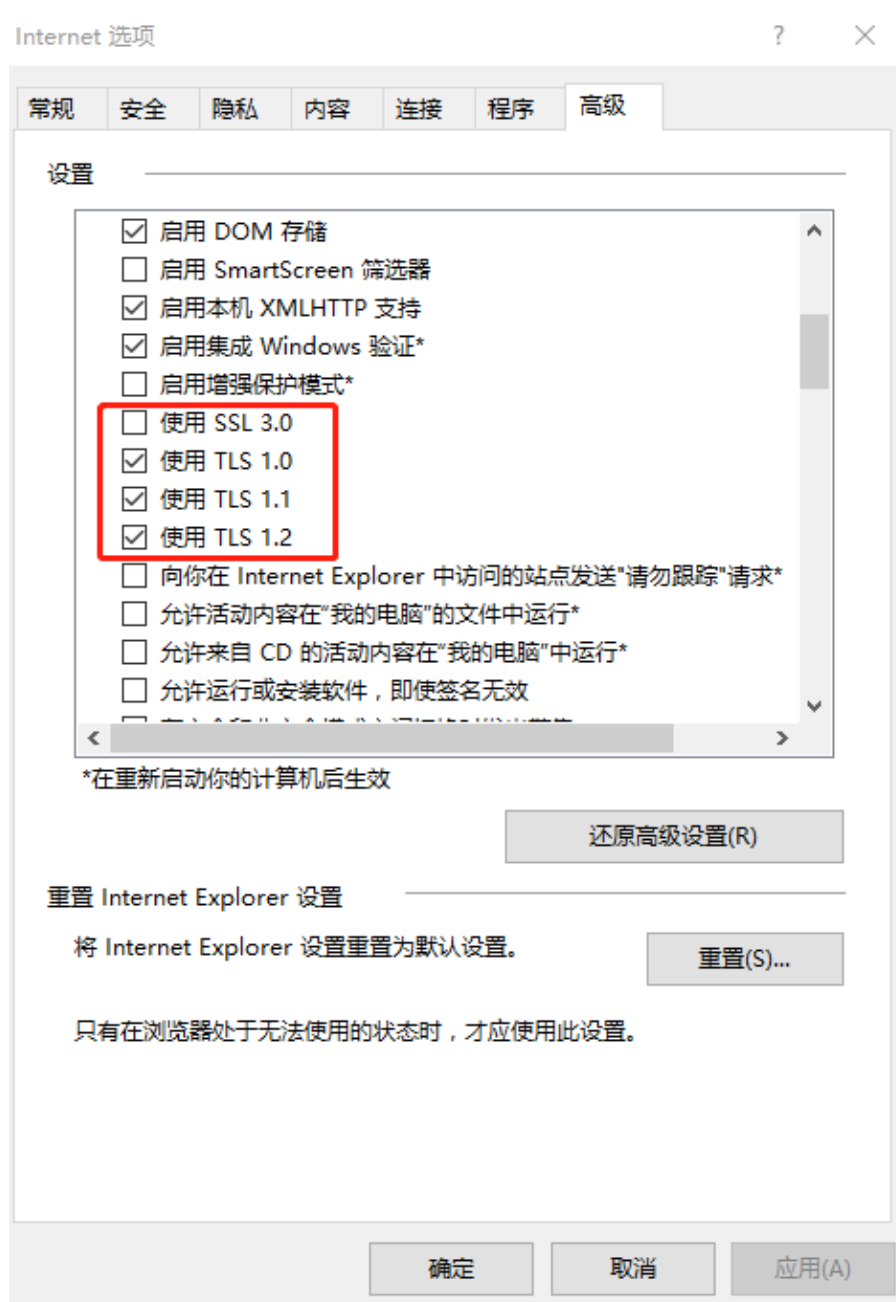
A screenshot of a user login form titled '用户登录'. The form contains three input fields: '用户名:' with the value 'sss', '密码:' with masked characters '\*\*\*\*\*', and '验证码:' with a value of '8513'. Below the verification code field, there is a small image showing the digits '6881'. At the bottom of the form, there are two buttons: '登录' (Login) and '重置' (Reset). Below the buttons, there is a red error message: '登录失败，用户名或密码错误' (Login failed, username or password error). At the very bottom, there is a disclaimer: '数字证书为用户身份的重要依据，请妥善保管。请勿将数字证书借给他人使用，以免造成信息安全风险。' (Digital certificate is an important basis for user identity, please妥善保管. Do not lend the digital certificate to others, to avoid information security risks.)

后续的登录及业务操作方法请见各业务系统客户端操作手册。

## 6 常见问题

### 6.1 证书选择框无法跳出

1. 检查浏览器版本是否符合要求，证书驱动是否已安装；
2. 若为 IE 浏览器，请查看 Internet 选项高级选项卡中，TLS1.0、TLS1.1、TLS1.2 是否已勾选，SSL3.0 是否已去掉勾选。



## 6.2 代理软件服务启动失败

若代理软件的 NC 安全无协议服务启动失败，

1. 检查代理软件是否被安装在网络磁盘上，代理软件需安装在本地磁盘上启动时才能获取足够的权限；
2. 检查本机的防火墙、杀毒安全软件等是否将代理软件加入了黑名单；
3. 完全关闭代理软件，打开 Windows 任务管理器，若存在残留进程则全部强制结束任务。

