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 或 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 2.跨浏览器插件（NetSignCNG） 3.代理软件（BiSafe）	地址：191.168.1.131 加密链路端口：7202 非加密链路端口：7203
2	CDS 系统	Windows7 或 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 2.跨浏览器插件（NetSignCNG） 3. 代理软件（BiSafe）	地址：191.168.1.155 加密链路端口：7212 非加密链路端口：7222
3	BDF 系统	Windows7 或 Windows10	CFCA 企业高级证书，通过证书	CFCA UKEY	IE11	1.UKEY 驱动 2.跨浏览器插件（NetSignCNG） 3. 代理软件	地址：191.168.1.150 端口：7855（会员）

			管理系统申请			（BiSafe）	、7844（代理客户）
4	FFA 系统	Windows7 或 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 2.跨浏览器插件（NetSignCNG） 3. 代理软件（BiSafe）	地址：191.168.1.135 端口：6666（清算会员、经纪公司）
5	BIS 系统	Windows7 或 Windows10	CFCA 企业高级证书，通过证书管理系统申请	CFCA UKEY	-	1.UKEY 驱动 2.招标发行系统承销商客户端 3.代理软件（BiSafe）	目的地址：191.168.1.137 端口：6556（承销商）、6555
6	CMS 系统	Windows7 或 Windows10	CFCA 企业高级证书，通过证书管理系统申请	CFCA UKEY	Chrome (84 及以下)	1.UKEY 驱动 2.跨浏览器插件（NetSignCNG） 3. 代理软件（BiSafe）	目的地址：191.168.1.170 端口： 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!”。

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。

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。

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

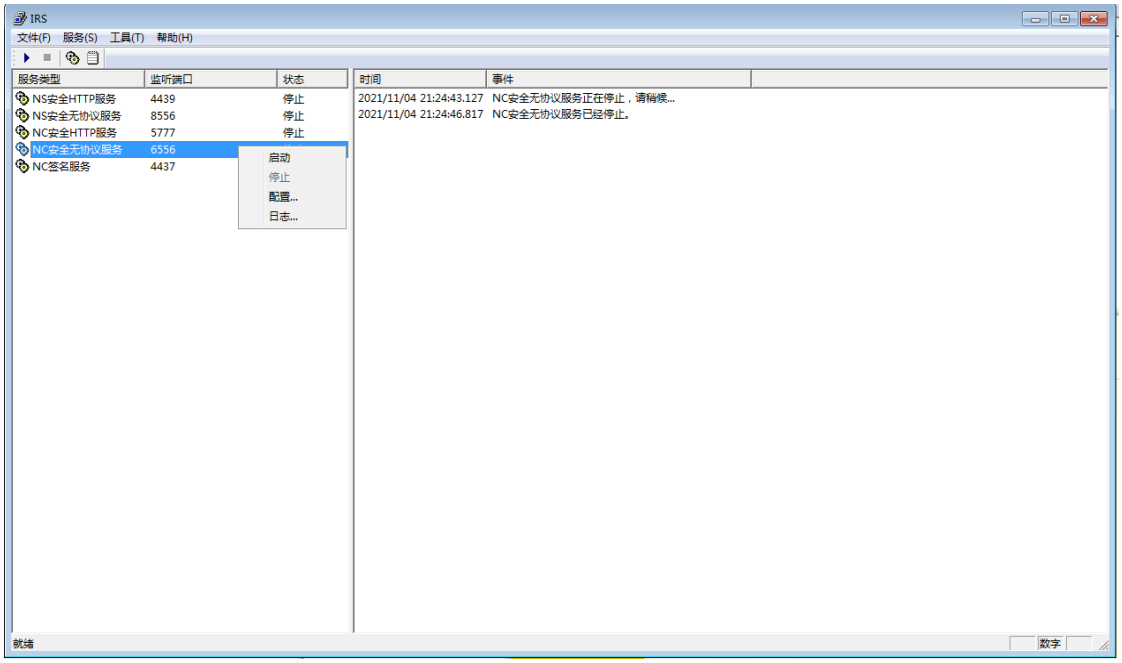
(1)创建 BiSafe 3.18 的安装目录，建议该目录创建在 C 盘根目录下或者 C:\Program Files(x86)目录下。

(2)解压 BiSafe318.zip 至安装目录。

(3)将 BiSafe.exe 快捷方式发送至桌面。

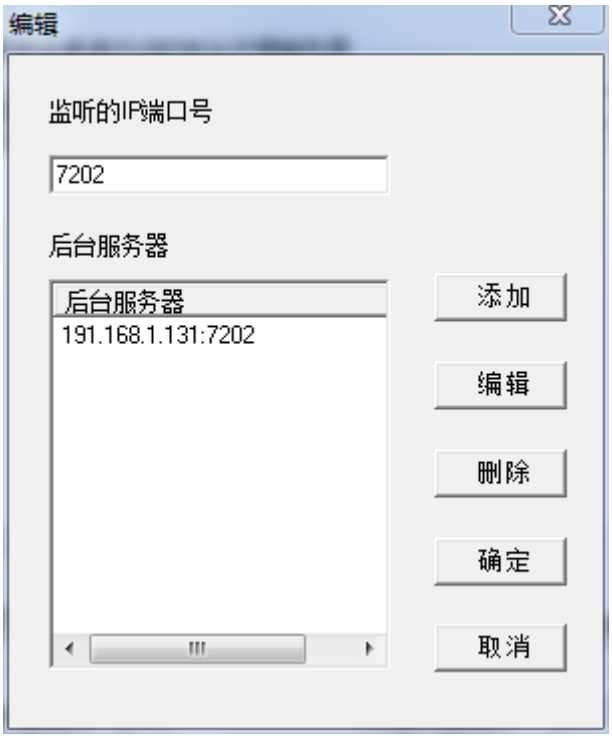
2.软件配置

(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

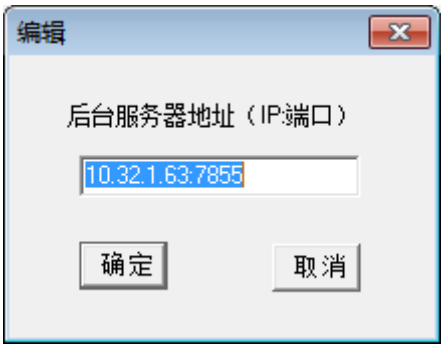


(2)在配置对话框中，选择“Server 配置”页，点击编辑

(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

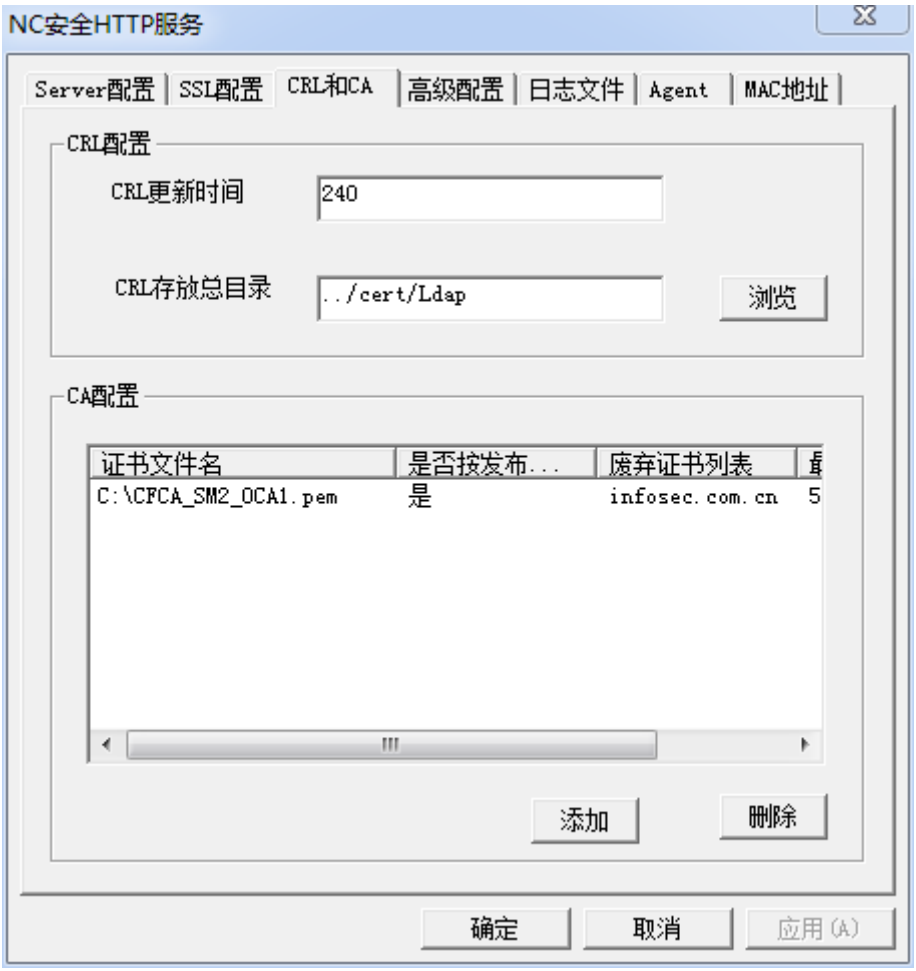
使用方式选择“使用硬方式”

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

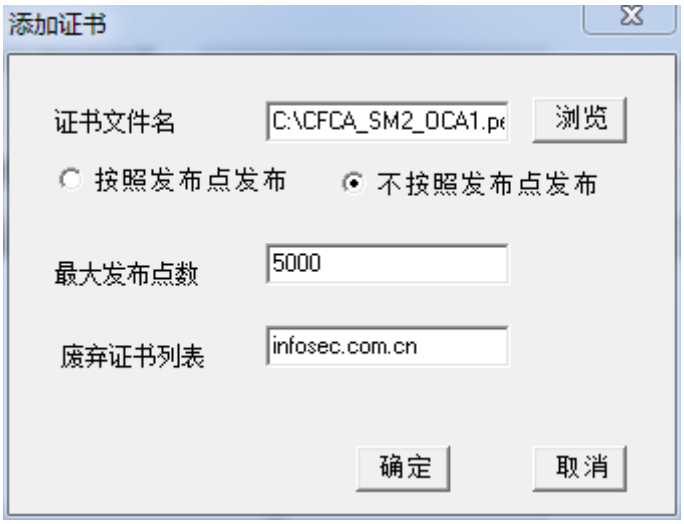
令牌的名称默认填：ShangHaiClearingHouse

(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[Crl]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） 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

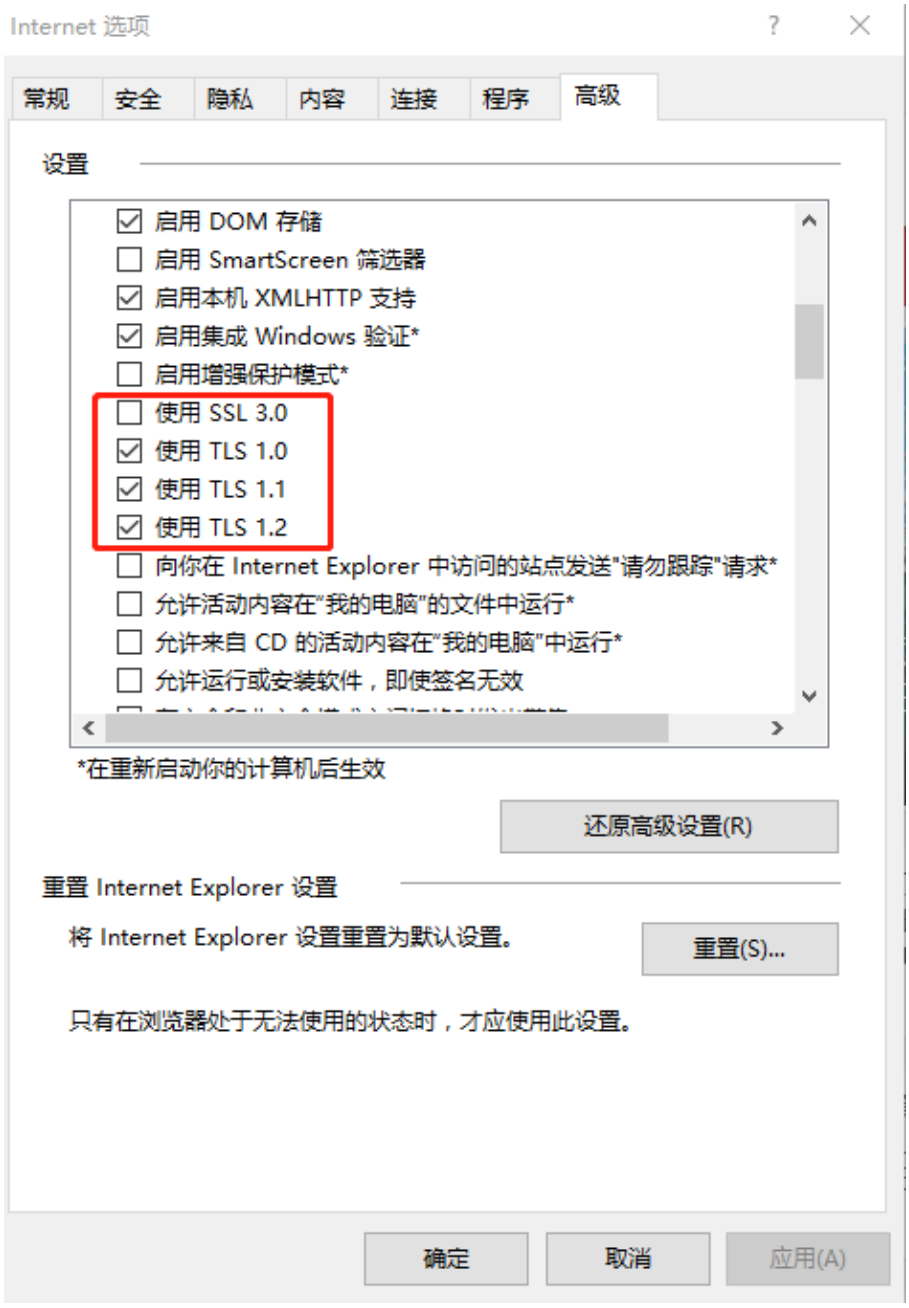
后续的登录及业务操作方法请见各业务系统客户端操作手册。

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。