期货公司客户交易终端
信息采集及接入认证技术规范

2018 年 9 月

中国期货市场监控中心　发 布

目　次

1　背景与范围 1

1.1 背景说明..... 1
1.2 适用范围..... 1

2　术语和定义 1

2.1 客户交易终端..... 1
2.2 交易软件..... 1
2.3 直连模式..... 1
2.4 中继代理模式..... 1
2.5 AppID/RelayAppID..... 1
2.6 授权码 2
2.7 交易软件厂商 ID..... 2

3　信息采集及接入认证概述..... 2

3.1 信息采集及接入认证流程..... 2
3.2 信息采集概述..... 2
3.3 接入认证概述..... 2

4　信息采集 3

4.1 采集指标术语解释..... 3
4.2 采集指标..... 4
4.3 采集方法..... 9
4.4 信息报送..... 11
4.5 信息安全要求..... 13

5　接入认证 14

5.1 认证方法..... 14
5.2 认证流程..... 14

附录 A （规范性附录） 16

A.1 加密密钥申请流程..... 16
A.2 信息处理示例..... 18

附录 B （参考性附录） 21

B.1 采集流程示例..... 21
B.2 认证流程示例..... 26
B.3 信息采集函数参考..... 28

1　背景与范围

1.1　背景说明

根据《关于加强证券期货经营机构客户交易终端信息等客户信息管理的规定》（证监会公告［2013］30号）的有关要求，为进一步加强期货市场看穿式监管要求，指导期货公司按要求规范其客户交易终端信息的采集、记录、存储和报送等工作，制订本技术规范。本技术规范将对期货公司客户交易终端信息的采集范围、采集标准和采集内容做出统一规定，以进一步促进交易终端信息规范化管理。

1.2　适用范围

本规范旨在明确各业务场景下需要采集的客户交易终端信息内容，限定客户交易终端信息的采集范围，统一客户交易终端信息记录与存储的格式要求，针对客户交易终端信息的采集、记录和存储过程给出明确的技术要求。

本规范的适用条件为通过期货公司入场交易的客户。适用范围包括客户交易终端的信息采集、交易终端与期货公司之间的信息通讯、期货公司内部的数据记录及期货公司与中国期货市场监控中心（以下简称监控中心）系统之间的信息通讯。

2　术语和定义

2.1　客户交易终端

客户交易终端是指客户下达交易指令的终端设备。其中，交易指令包括账户登录、交易委托、银期转账和密码修改等。

2.2　交易软件

本规范所称交易软件，是指能够接收、处理和转发客户交易指令到期货交易所（以下简称交易所）的软件，不包括客户交易终端软件。

2.3　直连模式

客户交易终端软件与期货公司交易软件直接通讯，进行交易的模式。

2.4　中继代理模式

客户交易终端软件与期货公司交易软件间接通讯，进行交易的模式。

本规范将客户交易终端软件和期货公司交易软件之间的通讯组件称为期货公司中继代理（以下简称中继代理）。

2.5　AppID/RelayAppID

AppID是客户交易终端软件的唯一标识码，由终端软件商按照规范要求编制，AppID由终端厂商名称、终端软件名称和版本号三部分构成。RelayAppID是中继代理软件的唯一标识码，由中继代理软件商按照规范要求编制，RelayAppID由中继厂商名称、中继软件名称和版本号三部分构成。

2.6 授权码

授权码由期货公司依据终端软件商或中继代理软件商提交的AppID或RelayAppID生成派发，用于AppID或RelayAppID的合法性校验。

2.7 交易软件厂商 ID

交易软件厂商ID是交易软件商的唯一标识，由交易软件商向监控中心申请加密密钥时同步获取。

3 信息采集及接入认证概述

3.1 信息采集及接入认证流程

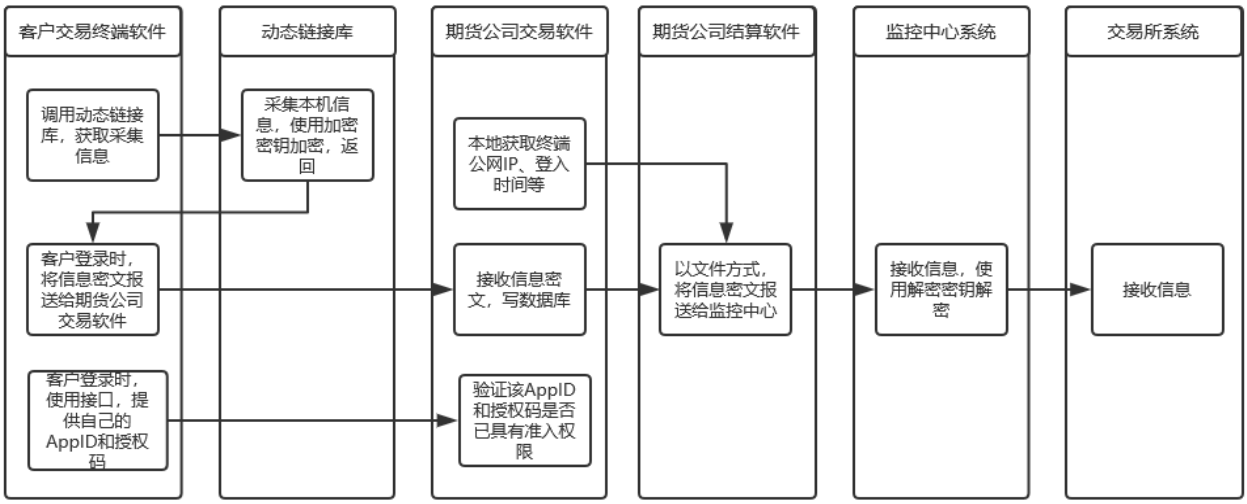


图3-1 信息采集及接入认证流程图

3.2 信息采集概述

a) 监控中心为每家交易软件商产生一对单独的非对称密钥，解密密钥由监控中心保存，加密密钥公开给交易软件商，集成在动态链接库中。
b) 交易软件商开发动态链接库，提供给终端软件商使用。由动态链接库主动采集客户交易终端信息并加密。
c) 终端软件登录时采集信息，并将信息密文即时报送给期货公司交易软件。
d) 交易软件在终端软件接入时补充获取其“交易软件厂商ID”、“公网IP”、“登入时间”和“客户内部资金账户”等，逐条填充至相应终端上报的信息数据中，汇总上报至结算软件。
e) 结算软件将信息密文报送给监控中心。
f) 监控中心系统解密密文。

3.3 接入认证概述

a) 期货公司组织对终端软件的接入认证，审查其软件功能，测试评估其是否已集成符合监管要求的信息采集动态链接库，是否能够准确采集客户终端信息。对于符合上述要求的终端软件，在交易软件中，配置其AppID和授权码，开通准入权限。
b) 客户使用交易终端软件登录时，携带交易终端软件的AppID和授权码，期货公司交易软件进行验证。

4　信息采集

4.1　采集指标术语解释

名词	解释
IP 地址	即互联网通讯协议地址（Internet Protocol Address），是指根据互联网协议为访问互联网的每台主机分配的一个逻辑地址。根据IP协议的不同版本，地址可分为IPV4和IPV6。
端口号	端口包括物理端口和逻辑端口。物理端口是用于连接物理设备之间的接口，逻辑端口是逻辑上用于区分服务的端口。本规范所指端口号为逻辑端口号。
MAC 地址	即媒介访问控制地址（Medium/Media Access Control），是指网络接口的物理地址，或称为硬件地址。在OSI模型和TCP/IP协议栈中，MAC地址分别对应于数据链路层和网络接口层，用于在该层进行信息转发。
设备名	是指客户对终端设备自定义的名字。
操作系统版本	管理和控制计算机硬件与软件资源的计算机程序，是直接运行在“裸机”上的最基本的系统软件，任何其他软件都必须在操作系统的支持下才能运行。本文所述的操作系统版本，特指发行版本。
CPU 序列号	即中央处理器 (Central Processing Unit)序列号，简称CPUID，包含该CPU的版本、主频、外频、二级缓冲等关键信息。
硬盘序列号	是指PC终端设备硬盘设备的编码，是用于标识硬盘产品信息的唯一识别码，一般包含生产地和生产日期等信息，不同厂商的硬盘产品具有不同的编码方法。
BIOS序列号	本规范所指BIOS序列号，是指计算机的BIOS芯片里的序列号。
分区信息	分区信息（PartitionInformation），是指对硬盘进行分区或格式化处理后产生的与分区相关的信息，包括盘符、分区序列号、分区格式、分区容量等参数。其中，分区序列号是指分区时自动生成的分区标识信息，由一串十六进制字符组成，常见的分区格式有FAT、FAT32、NTFS等。
设备序列号	是指设备的唯一标识。PC端是指MAC OS系统的终端设备序列号，移动端是指移动终端的序列号。
网络运营商	网络运营商是进行网络运营和提供服务的实体。网络运营商不仅需要从网络角度知道网络运行状况，还需要从服务角度知道网络运行状况。
设备类型	本规范所指移动终端设备类型，是指“pad”，“pod”，“phone”等。
地理位置信息	以经纬度为度量标准的绝对地理位置信息。
UUID	即通用唯一识别码(UniversallyUnique Identifier)，是指广泛应用在分布式计算环境中用来标识存储设备的编码，由一串十六进制字符串组成。
IMEI	即国际移动设备识别码（International Mobile Equipment Identity），是区别移动设备的标志。GSM和WCDMA手机终端使用该码。
MEID	即移动设备识别码(Mobile Equipment Identifier)，是CDMA手机的身份识别码，也是每台CDMA手机或通讯平板唯一的识别码。
IMSI	是区别移动用户的标志，储存在SIM卡中，可用于区别移动用户的有效信息。

ICCID	ICCID为IC卡的唯一识别号码，共有20位数字组成，其编码格式为：XXXXXX OMFSS YYGXX XXXX。
微信OpenID	是指微信用户在微信公众号中的唯一识别码，通过微信OpenID可查询到客户的姓名、昵称、头像、性别、城市等信息。
异常标识	本规范中是指信息采集和获取的过程中，出现可识别异常后，按编码规则要求填写的错误代码。
用户类型	本规范中是指区分下单客户身份类型的标识。
操作员	在期货公司交易软件内，为若干具备交易编码的客户代理下单的角色。

4.2 采集指标

4.2.1 终端采集指标

在信息采集过程中，按照客户交易终端信息的重要程度及技术可行性,针对于不同的平台，设定了不同的采集内容，所有内容均需要采集。

客户交易终端设备按照类型可分为PC终端、移动终端和其他终端。

a) PC终端分为Windows、Linux、Mac OS等操作系统版本。

b) 移动终端分为iOS、Android等操作系统版本。

c) 其他终端分为微信、线下委托等。

4.2.1.1 PC 端采集指标

PC终端包括PC应用程序和浏览器,其中浏览器需要通过必要的技术手段保证终端信息的采集，如加载经过认证的插件等。

各种操作系统需要采集的内容如下表：

操作系统	Windows	Linux	Mac OS
采集指标	信息采集时间 私网IP 网卡MAC地址 设备名 操作系统版本 硬盘序列号 CPU序列号 BIOS序列号 系统盘分区信息	信息采集时间 私网IP 网卡MAC地址 设备名 操作系统版本 硬盘序列号 CPU序列号 BIOS序列号	信息采集时间 私网IP 网卡MAC地址 设备名 操作系统版本 硬盘序列号 设备序列号

4.2.1.2 移动终端采集指标

移动终端包括移动应用程序和浏览器,其中浏览器需要通过必要的技术手段保证终端信息的采集，如加载经过认证的插件等。

各种操作系统需要采集的内容如下表：

操作系统	iOS	Android
采集指标	信息采集时间 移动终端IP 地理位置信息 操作系统版本	信息采集时间 移动终端IP 地理位置信息 操作系统版本

	设备名 设备类型 网络运营商 通用唯一识别码（UUID）	设备名 设备类型 国际移动设备识别码（IMEI） 移动设备识别码（MEID） 设备MAC地址 手机号码 设备序列号 国际移动用户识别码（IMSI） IC卡的唯一识别号码（ICCID）

4.2.1.3 其他终端采集指标

其他业务类型需要采集的内容如下表：

业务类型	线下委托	微信委托
采集指标	信息采集时间（线下委托时间） 电话号码（客户电话号码）	信息采集时间 OpenID 地理位置信息
补充说明	通过电话、邮件、QQ及各类通讯工具在线下传达下单通知的，需要采集客户的电话号码。	无

4.2.2 补充获取指标

4.2.2.1 直连模式获取指标

获取位置	交易软件
获取指标	交易软件厂商ID（从交易软件获取） 加密密钥版本（从终端获取） 异常标识（从终端获取，可本地重置） AppID（从终端获取） 客户交易终端公网IP（从交易软件获取） 客户交易终端公网端口号（从交易软件获取） 客户交易终端登入时间（从交易软件获取） 客户内部资金账户（从交易软件获取） 用户类型（从交易软件获取）

4.2.2.2 中继代理模式获取指标

a) 中继代理

获取位置	中继代理
获取指标	加密密钥版本（从终端获取，转发） 异常标识（从终端获取，可本地重置） AppID（从终端获取，转发） 客户交易终端公网IP（从中继代理获取，转发） 客户交易终端公网端口号（从中继代理获取，转发） 客户交易终端登入时间（从中继代理获取，转发）

b) 交易软件

获取位置	交易软件
获取指标	交易软件厂商ID（从交易软件获取） 加密密钥版本（中继代理获取） 异常标识（从中继代理获取，可本地重置） AppID(从中继代理获取) 客户交易终端公网IP（从中继代理获取） 客户交易终端公网端口号（从中继代理获取） 客户交易终端登入时间（从中继代理获取） RelayAppID(从中继获取) 中继代理公网IP（从交易软件获取，获取交易软件下一级中继） 中继代理公网端口号（从交易软件获取，获取交易软件下一级中继） 中继代理登入时间（从交易软件获取，获取交易软件下一级中继） 客户内部资金账户（从交易软件获取） 用户类型（从交易软件获取）

4.2.3 类型信息编码

a) 在终端信息字符串中，终端类型编码约定如下表所示：

终端类型	终端类型编码
Windows终端	‘1’
Linux终端	‘2’
Mac OS终端	‘3’
移动iOS终端	‘4’
移动Android终端	‘5’
线下委托终端	‘6’
微信终端	‘7’

b) 在操作员为客户下单的模式中，补充获取信息中用户类型填写为操作员，用户类型编码约定如下表所示：

用户类型	用户类型编码
客户	‘1’
操作员	‘2’

c) 在终端信息字符串中，异常标识编码约定如下表所示：

异常标识类型	异常标识编码
正常	‘0’
终端信息采集为空	‘1’
终端采集数据加密密钥版本异常	‘2’
终端信息数据异常	‘3’

4.2.4 采集指标格式

终端设备名称等超长信息，其长度大于限定字节数时，按照要求截取字符串前N个字节为信息字符串。终端信息字符串中各个指标信息最大长度（单位：字节）说明如下：

终端类型	
最大长度	1
信息示例	1
信息采集时间	
最大长度	19
信息示例	2018-05-01 09:00:00（统一为东八区时间）
IP地址	
最大长度	39
信息示例	192.168.123.123
信息示例	CDCD:910A:2222:5498:8475:1111:0010:2020
特殊说明	1. PC终端信息中的私网IP地址默认获取2个，应首选采集处于激活状态的网卡信息。 2. 补充获取时，对于没有公网IP的，采集其专线IP。 3. IP 地址处理要求。IPV4 地址以“点分十进制” 表示x.x.x.x 的形式记录。IPV6 地址以“冒号分十六进制”表示为n: n: n: n: n: n: n: n 的形式记录，n 表示四个十六位地址元素之一的十六进制值，可采用“零压缩法（如果几个连续段位的值都是0，那么这些0就可以简单的以::来表示）”的形式记录。
端口号	
最大长度	5
信息示例	1025
MAC地址	
最大长度	12
信息示例	005056C00008
特殊说明	1. PC终端信息中的MAC地址默认获取2个，应首选采集处于激活状态的网卡信息。 2. 移动端用户需要开通授权。 3. MAC地址处理要求。MAC地址去掉地址中的‘-’或‘：’进行记录。
设备名	
最大长度	9
信息示例	cfmmc.pc
特殊说明	设备名为超长信息，其长度大于限定字节数时，需要注意截取处应避免出现汉字被截断的情况。
操作系统版本	
最大长度	5
信息示例	10.0*
CPU序列号	
最大长度	16
信息示例	BFEBFBFF000406E3
特殊说明	多颗CPU情况下，采集物理编号为0的CPU信息。

硬盘序列号	
最大长度	16
信息示例	86D6C8Z6T
系统盘分区信息	
最大长度	24
信息示例	C,201C3A22,FAT32,80
特殊说明	系统盘分区信息（只记录承载操作系统的磁盘信息）包括：盘符、分区序列号、分区格式、分区容量(G)，各信息间以逗号隔，即“盘符，分区序列号，分区格式，分区容量”。
BIOS序列号	
最大长度	10
信息示例	PC0CJEY5
设备序列号	
最大长度	12
信息示例	C02RY79KF43V
网络运营商	
最大长度	12
信息示例	中国移动
设备类型	
最大长度	12
信息示例	phone
地理位置信息	
最大长度	17
信息示例	N35.461,E111.362
特殊说明	1. 需要用户开通授权 2. 北纬用“N”表示，南纬用“S”表示，东经用“E”表示，西经用“W”表示。 3. 小数点后保留三位有效数字。
IMEI	
最大长度	15
信息示例	869011025656751
特殊说明	需要用户开通授权
MEID	
最大长度	14
信息示例	86901102568765
特殊说明	需要用户开通授权
手机号码	
最大长度	11
信息示例	13800000000

特殊说明	1. 需要用户开通授权 2. 仅安装一张SIM卡时，采集已安装SIM卡的手机号。安装两张卡时，采集SIM1卡的手机号。
UUID	
最大长度	32
信息示例	E39DC982705E5B008C13AFDE0DF2FEA1
IMSI	
最大长度	15
信息示例	460026102456666
特殊说明	1. 需要用户开通授权 2. 仅安装一张SIM卡时，采集已安装SIM卡的IMSI。安装两张卡时，采集SIM1卡的IMSI。
ICCID	
最大长度	20
信息示例	898600f10115f0172111
特殊说明	1. 需要用户开通授权 2. 安装一张SIM卡时，采集已安装SIM卡的ICCID。安装多张卡时，采集编号最小的SIM卡的ICCID。
电话号码	
最大长度	20
信息示例	0838-65255555-1234
微信OpenID	
最大长度	28
信息示例	eb429b100968f2c0ef38
客户内部资金账户	
最大长度	18
信息示例	000100000001

注：空格处理要求。单个终端信息中有多个空格时，需处理为单个空格；单个终端信息的起始和结尾不能包含空格。

4.3 采集方法

4.3.1 采集原则

客户交易终端信息是登录信息的重要组成部分。**为兼顾运行效率和采集准确性，仅在客户每次登录时采集客户交易终端信息。**对于线下委托和微信委托在下达交易指令时，进行信息采集。

4.3.2 采集流程

4.3.2.1 直连模式采集流程

直连模式交易终端信息采集的业务流程如下图所示：

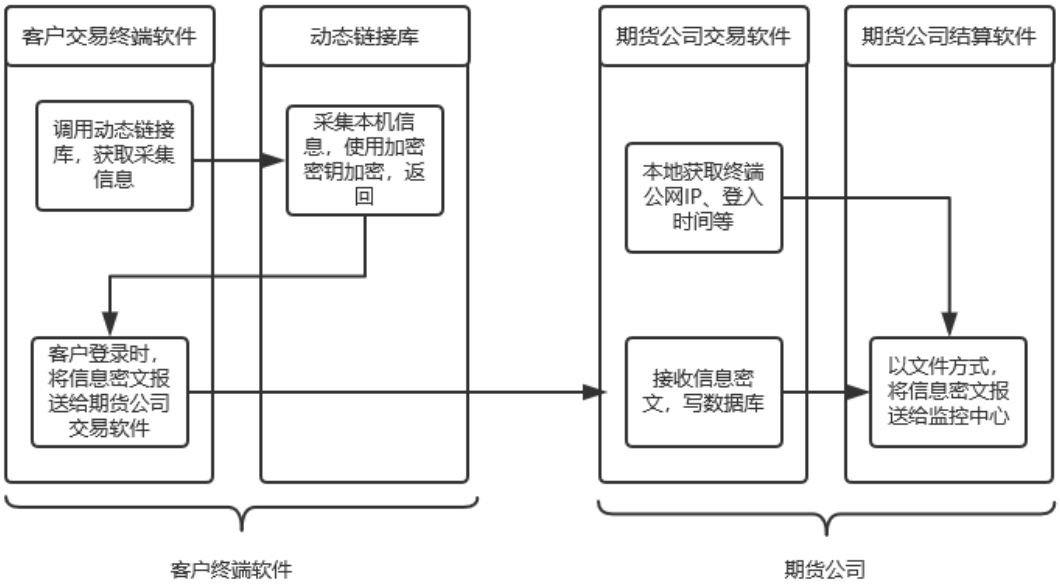


图4-1 信息采集业务流程

a) 交易软件商向监控中心发起获取加密密钥的正式申请，监控中心审核身份通过后，派发加密密钥。

b) 交易软件商开发动态链接库，提供给终端软件商使用。动态链接库负责采集客户交易终端信息，并使用加密密钥对采集信息进行整体加密，如果信息采集失败则应返回相应错误信息。

c) 终端软件商将信息采集动态链接库集成至终端软件，实现客户登录时采集终端信息，并将信息密文即时报送期货公司交易软件。如因权限问题，采集终端信息失败，则应提示用户开启信息采集的相应权限。

d) 交易软件在终端软件接入时补充获取“交易软件厂商ID”、“加密密钥版本”、“异常标识”、“AppID”、“客户交易终端公网IP”、“客户交易终端公网端口号”、“客户交易终端登入时间”、“客户内部资金账户”和“用户类型”，对相应指标进行加密，并汇总至结算软件。

e) 结算软件盘后将信息密文报送给监控中心。

f) 监控中心系统使用解密密钥解密密文。

4.3.2.2 中继代理模式采集流程

中继代理模式交易终端信息采集的业务流程如下图所示：

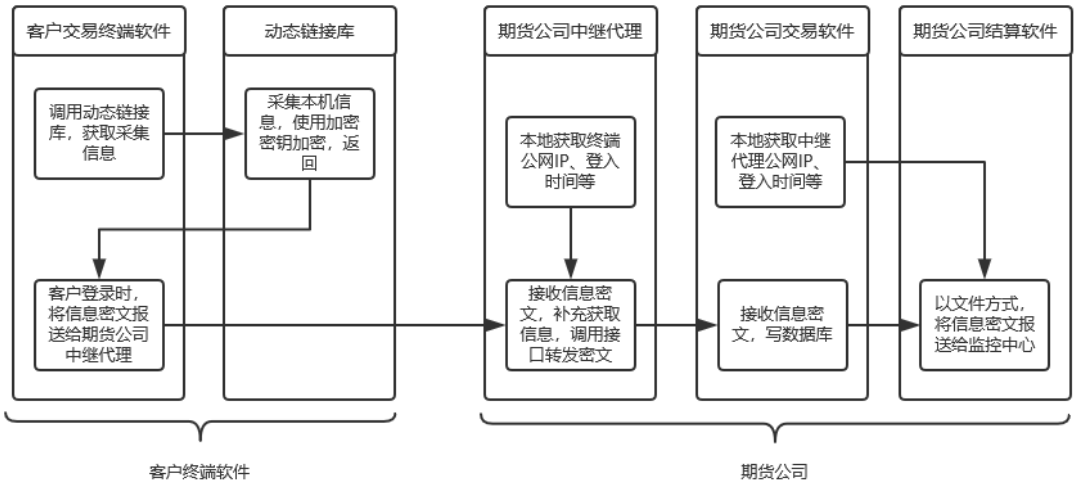


图4-2 信息采集业务流程

a) 交易软件商向监控中心发起获取加密密钥的正式申请，监控中心审核身份通过后，派发加密密钥。

b) 交易软件商开发动态链接库，提供给终端软件商使用。动态链接库负责采集客户交易终端信息，并使用加密密钥对采集信息进行整体加密。如果信息采集失败则应返回相应错误信息。

c) 交易软件商开发终端信息上报接口，提供给中继代理商使用。中继代理通过上报接口将客户交易终端采集信息，上报给期货公司交易软件。

d) 终端软件商将信息采集动态链接库集成至终端软件，实现客户登录时采集终端信息，并将信息密文即时报送期货公司中继代理。如因权限问题，采集终端信息失败，则应提示用户开启信息采集的相应权限。

e) 中继代理补充获取终端软件“异常标识”、“AppID ”、“客户交易终端公网IP”、“客户交易终端公网端口号”和“客户交易终端登入时间”，并将补充获取信息和终端上报信息发送给期货公司交易软件。

f) 交易软件在中继代理接入时补充获取“交易软件厂商ID”、“加密密钥版本”、“异常标识”、“RelayAppID”、“中继代理公网IP”、“中继代理公网端口号”、“中继代理登入时间”、“客户内部资金账户”和“用户类型”，对相应指标进行加密，并汇总至结算软件。

g) 结算软件盘后将信息密文报送给监控中心。

h) 监控中心系统使用解密密钥解密密文。

4.4 信息报送

4.4.1 报送原则

a) 信息采集数据应满足向监管机构报送要求，存储于交易软件中，每天盘后由主席结算软件把主次席的报送信息汇总成统一文件后，进行上报，监控中心收到文件后进行解密，并共享给相应交易所。生成的信息采集数据报送文件字符集为UTF-8，生成的报送文件名称格式为“期货公司统一标识clientinfo日期.txt”。

b) 采集指标应以统一的顺序和格式组装成信息采集字符串，并以RSA 2048 PKCS#1方式进行加密，为了兼顾后期替换为国密算法，软件商在开发时应保留一定的兼容性。加密后，使用BASE64方式进行转码，转码后的数据需要禁止出现换行符。

c） T-1日15:30至T日15:30的信息采集数据，应于T日报送。信息采集数据于每交易日与“期货保证金监控系统数据”一同报送。

4.4.2 报送格式

终端采集字符串由“终端采集指标”按一定顺序以英文符号“@”分隔拼接构成，并使用加密密钥进行加密。除“交易软件厂商ID”和“加密密钥版本”外，补充获取字符串由“补充获取指标”按一定的顺序以英文符号“@”分隔拼接构成，并由交易软件使用加密密钥进行加密。

终端采集字符串和补充获取字符串格式如下图：

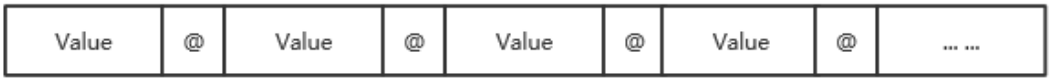


图4-3 终端采集字符串和补充获取字符串格式

信息采集数据由“交易软件厂商ID”、“加密密钥版本”、“终端采集信息密文”和“补充获取信息密文”组成，其中“终端采集信息密文”和“补充获取信息密文”需要先进行BASE64转码，转码后再按顺序以一定格式拼接。

信息采集数据格式如下图：

图4-4 信息采集数据格式

信息采用英文符号“@”分隔各采集指标。中继代理和交易软件本地另行获取的补充指标，由交易软件将其填充至相应上报信息数据中，汇总至结算软件。

根据终端设备类型的分类，各类型终端设备的详细信息整个字符串的描述顺序分别约定如下表所示：

终端设备类型	详细终端设备信息采集内容及记录顺序
Windows	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@私网IP1@私网IP2@网卡MAC地址1@网卡MAC地址2@设备名@操作系统版本@硬盘序列号@CPU序列号@BIOS序列号@系统盘分区信息@异常标识@AppID@客户交易终端公网IP@客户交易终端公网端口号@客户登入时间@RelayAppID@中继代理公网IP@中继代理公网端口号@中继代理登入时间@客户内部资金账户@用户类型
Linux	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@私网IP1@私网IP2@网卡MAC地址1@网卡MAC地址2@设备名@操作系统版本@硬盘序列号@CPU序列号@BIOS序列号@异常标识@AppID@客户交易终端公网IP@客户交易终端公网端口号@客户登入时间@RelayAppID@中继代理公网IP@中继代理公网端口号@中继代理登入时间@客户内部资金账户@用户类型
Mac OS	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@私网IP1@私网IP2@网卡MAC地址1@网卡MAC地址2@设备名@操作系统版本@硬盘序列号@设备序列号@异常标识@AppID@客户交易终端公网IP@客户交易终端公网端口号@客户登入时间@RelayAppID@中继代理公网IP@中继代理公网端口号@中继代理登入时间@客户内部资金账户@用户类型

iOS	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@移动终端IP@地理位置信息@操作系统版本@设备名@设备类型@网络运营商@UUID@异常标识@AppID@客户交易终端公网IP@客户交易终端公网端口号@客户登入时间@RelayAppID@中继代理公网IP@中继代理公网端口号@中继代理登入时间@客户内部资金账户@用户类型
Android	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@移动终端IP@地理位置信息@操作系统版本@设备名@设备类型@IMEI1@IMEI2@MEID@设备Mac地址@手机号码@设备序列号@IMSI@ICCID@异常标识@AppID@客户交易终端公网IP@客户交易终端公网端口号@客户登入时间@RelayAppID@中继代理公网IP@中继代理公网端口号@中继代理登入时间@客户内部资金账户@用户类型
线下	交易软件厂商ID@加密密钥版本@终端类型@信息采集时间@电话号码@客户内部资金账户@用户类型
微信	交易软件厂商ID@加密密钥版本@终端类型@终端采集时间@OpenID@地理位置信息@客户内部资金账户@用户类型

注：

a) 标有底色的字段需要使用加密密钥进行加密，并BASE64转码。

b) 交易软件使用的加密密钥应与动态链接库的加密密钥一致。

4.4.3 特殊情况说明

为保证信息存储、解读的一致性，对详细终端信息格式可能面临的一些特殊情况的说明限定如下：

a) 空指标处理要求。终端采集指标或补充获取指标，出现异常情况指标为空时，需要保留分隔符。举例：格式为“终端类型@信息采集时间@移动终端IP”，当信息采集时间为空时，拼接字符串为“终端类型@@移动终端IP”。

b) 分隔符及转换处理要求。终端信息字符串各个信息之间以英文符号‘@’作为分割符,第一个信息前和最后一个信息后无分割符。当获取的某个终端信息中包含有‘@’分隔符时，使用“&at”进行转义替换。终端信息字符串解析时会根据转换规则还原对应信息，避免字符串解析错误。

4.5 信息安全要求

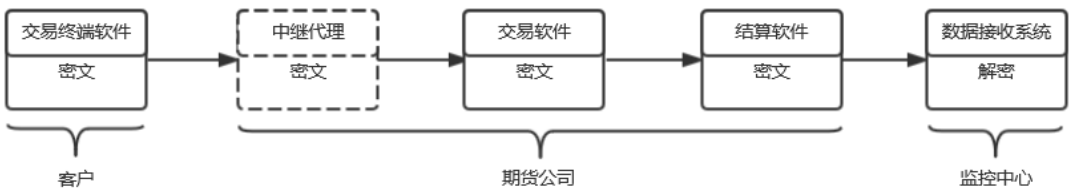


图4-5 信息采集安全要求

在整个终端信息传输及存储的过程中，要求如下：

a) 数据流从交易终端到中继代理，中继代理到交易软件，应采用高安全性，稳定性的传输协议，确保传输通道的安全性。同时，终端信息在传输过程中，应对终端信息数据本身采取一定安全措施，以进一步加强数据的安全性。

b) 为了数据的安全性，信息采集过程中，交易软件商应采取二次加密、密钥混淆等安全措施，加强对加密密钥的保护（禁止将密钥写入JAR中）。数据在交易软件数据库或结算软件报送文件等存储系统中，需要以密文的形式存储。

5 接入认证

5.1 认证方法

5.1.1 认证原则

a) 期货公司应负责组织对终端软件的功能核验及身份认证。期货公司需要测试评估终端软件是否已集成符合监管要求的信息采集动态链接库，是否能够准确采集客户终端信息。

b) 对于直接连接交易软件的终端软件，在交易软件中根据核验的结果设置终端软件的准入权限；对于通过中继代理连接交易软件的终端软件，在交易软件中根据核验的结果设置中继代理的准入权限，在中继代理中设置终端软件的准入权限。

c) 由于 AppID 与 RelayAppID 是由终端与中继厂商按照技术规范的要求编制后，上报给期货公司的唯一标识码。期货公司在组织功能核验时，需要审核终端厂商与中继厂商是否符合技术规范。不同终端软件或中继代理的 AppID/RelayAppID 在同一期货公司内部不允许重复。同一款终端软件或中继代理的 AppID/RelayAppID 在不同的期货公司应保持一致。

5.1.2 格式规范

AppID和RelayAppID格式约定如下表所示：

字段名称	终端/中继厂商名称	终端/中继软件名	版本号
最大长度	10	10	8
格式	终端/中继厂商名称_终端/中继软件名称_版本号		
示例	abcdef_ghijkl_1.6.0		
特殊说明	个人开发的终端软件 ，厂商名称为client。		

5.2 认证流程

5.2.1 采集功能核验

a) 直连模式

1) 客户交易终端厂商向期货公司发起认证申请。
2) 终端厂商根据规范要求编制AppID，上报期货公司。
3) 期货公司依据AppID发放授权码，终端厂商将其集成至终端软件。
4) 期货公司审核客户交易终端功能，对于符合监管规定的终端软件，在交易软件中，配置其AppID和授权码，开通准入权限。
5) 终端软件应具有提示用户开通相关信息采集权限的功能，并具有若用户不开通相关权限可禁止用户登录的功能。

b) 中继代理模式

1) 终端厂商联合中继代理厂商向期货公司发起认证申请。
2) 终端厂商根据规范要求编制AppID，中继代理厂商根据规范要求编制RelayAppID，上报期货公司。
3) 期货公司依据AppID和RelayAppID分别发放授权码，终端厂商和中继代理厂商将其分别集成至终端软件和中继代理中。
4) 期货公司审核中继代理功能，对于符合监管规定的中继代理，**在交易软件中，配置其RelayAppID和授权码，开通准入权限。**

5) 期货公司审核客户交易终端功能，对于符合监管规定的终端软件，**在中继代理中，配置其AppID和授权码，开通准入权限。**

6) 终端软件应具有提示用户开通相关信息采集权限的功能，并具有若用户不开通相关权限可禁止用户登录的功能。

5.2.2 接入身份认证

a) 直连模式

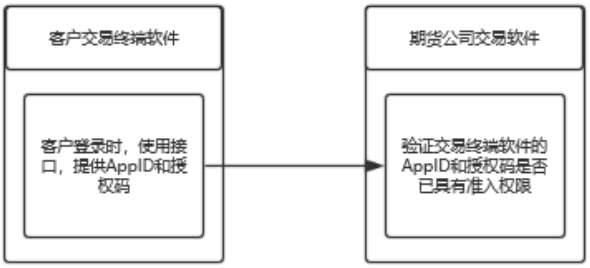


图5-1 终端认证业务流程图

客户交易终端软件登录时，携带其AppID和授权码，连接期货公司交易软件，认证通过后，方可登录交易软件。

此外，考虑到客户交易终端软件接入认证功能需要明文使用AppID，该指标从终端采集无需加密，由交易软件统一进行加密操作。

b) 中继代理模式

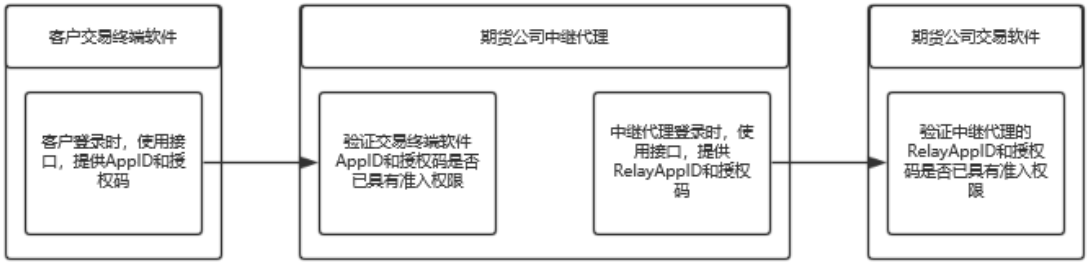


图5-2 终端认证业务流程图

客户交易终端软件携带AppID和授权码，连接期货公司中继代理，认证通过后，方可登录中继代理。

中继代理软件携带RelayAppID和授权码，连接期货公司交易软件，认证通过后，方可登录交易软件、上报终端采集信息。

此外，考虑到客户交易终端软件和中继代理接入认证功能需要明文使用AppID和RelayAppID，该两项指标从终端和中继代理采集无需加密，由交易软件统一进行加密操作。

附 录 A
（规范性附录）

A.1 加密密钥申请流程

a) 交易软件商登录https://softwarevendor.cfmmc.com申请账号，并按照系统提示填写相应信息（附件1），申请获取信息采集加密密钥、加密密钥版本、交易软件厂商ID及信息采集函数名信息。（为避免动态链接库函数名重复，建议命名规则为“交易软件厂商ID_getsysteminfo”）

b) 监控中心核验交易软件商身份，交易软件商需要按要求配合提供纸质材料，身份核验通过后，由监控中心执行系统操作进行信息派发。交易软件商按照指定的安全方式获取加密密钥、加密密钥版本、交易软件厂商ID及信息采集函数名信息。

c) 如交易软件商需要重发密钥或撤销密钥，可登录https://softwarevendor.cfmmc.com申请。

d) 交易软件商应保管好自己的加密密钥，防止加密密钥泄露。交易软件商成功获得加密密钥后，1年内不得重新申请新加密密钥；每次重新申请新加密密钥，旧加密密钥将于1年后失效。交易软件商在任何时间的有效加密密钥最多不可以超过2个。

e) 交易软件商的联系方式是接收加密密钥的重要途径，当公司基本信息与人员基本信息发生变更时，交易软件商应及时登录https://softwarevendor.cfmmc.com进行信息变更。

附件 1.

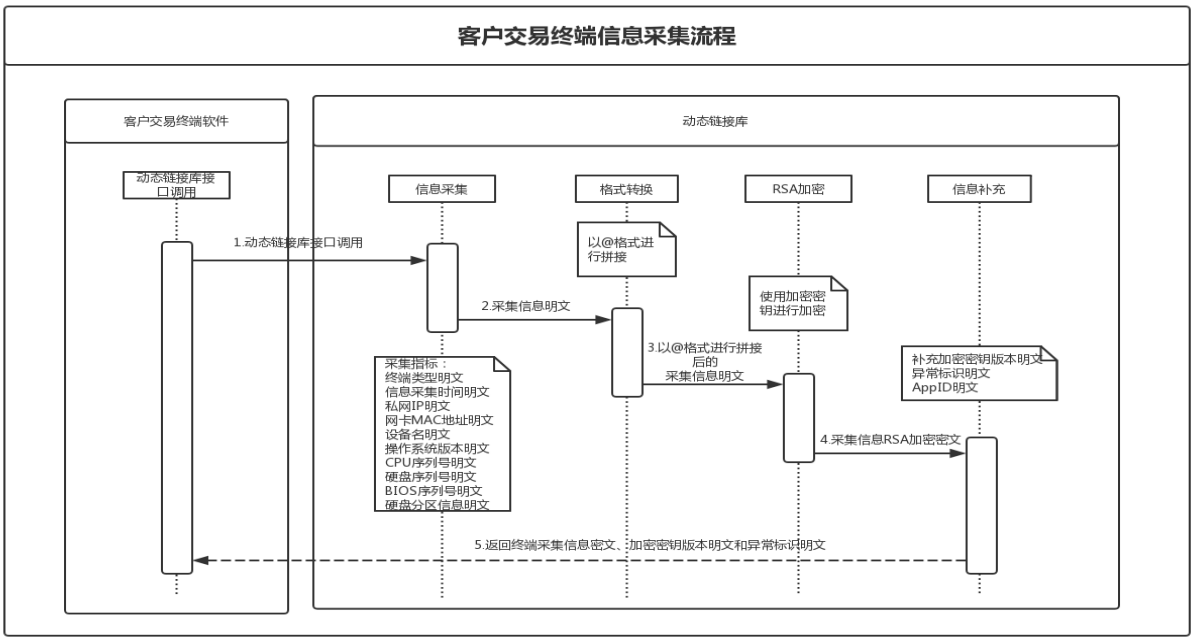
公司基本信息	
*统一社会信用代码	
*单位全称（中文）	
单位简称（中文）	
*单位全称（英文）	
*单位简称（英文）	
单位类型	☐独立软件供应商 ☐会员单位 ☐其他_____
单位注册地址	
*已接入交易所	☐上海期货交易所 ☐郑州商品交易所 ☐大连商品交易所 ☐中国金融期货交易所 ☐上海国际能源交易中心
人员基本信息	
技术负责人信息	
*姓名	
职务	
*电子邮件	
*手机号码	
工作联系人信息	
*姓名	
座机号码	
*手机号码	
*电子邮件	

注：标*为必填项，各交易软件商应准确填写相关信息，避免因信息有误影响加密密钥及厂商ID的申请工作。

A.2 信息处理示例（以 Windows 为例）

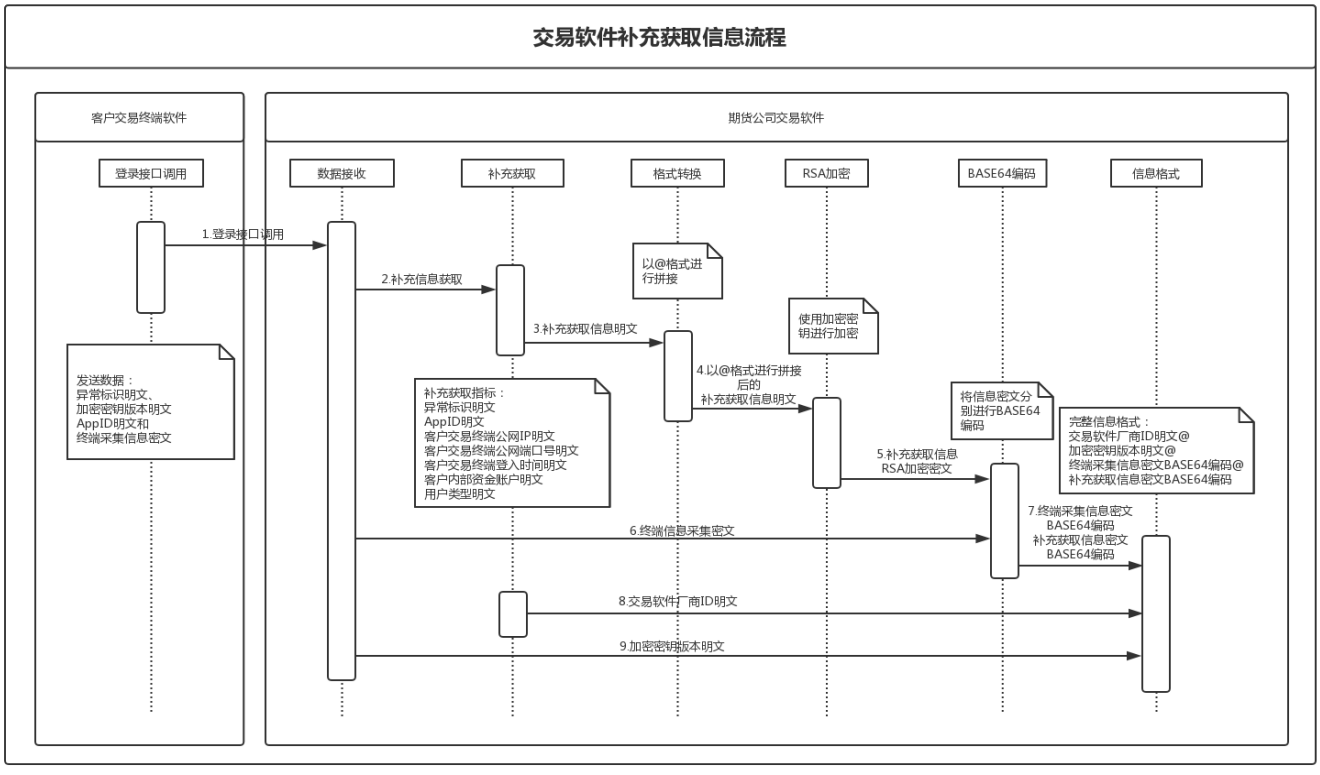
a） 直连模式

1） 客户交易终端



图A-1 客户交易终端信息采集流程

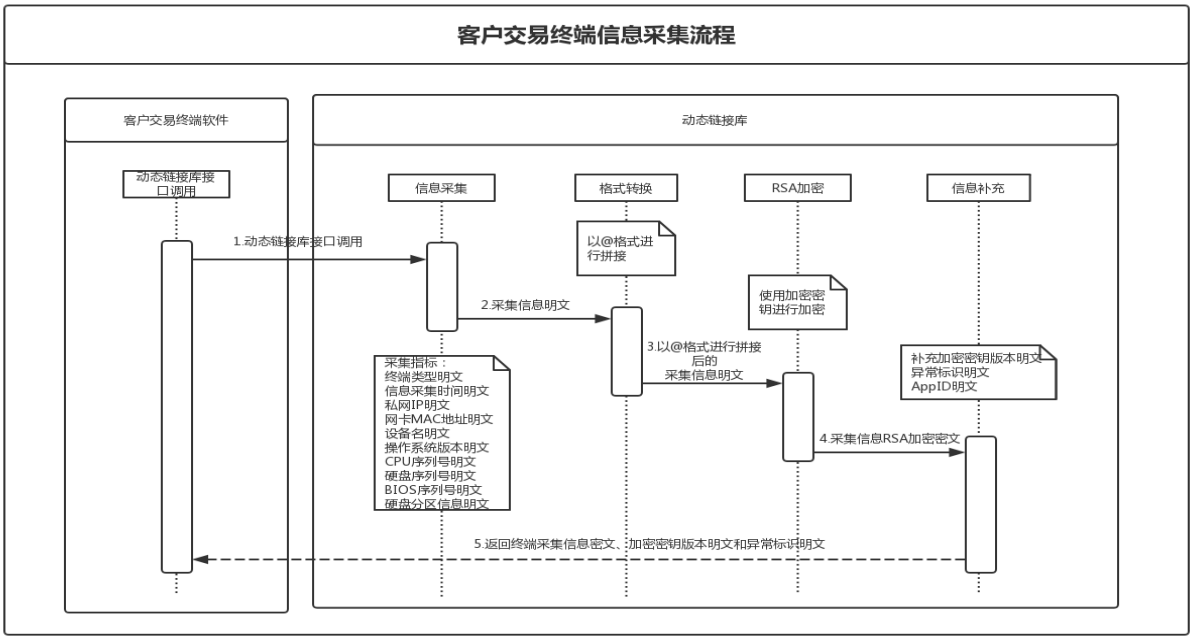
2） 期货公司交易软件



图A-2 期货公司交易软件信息处理流程

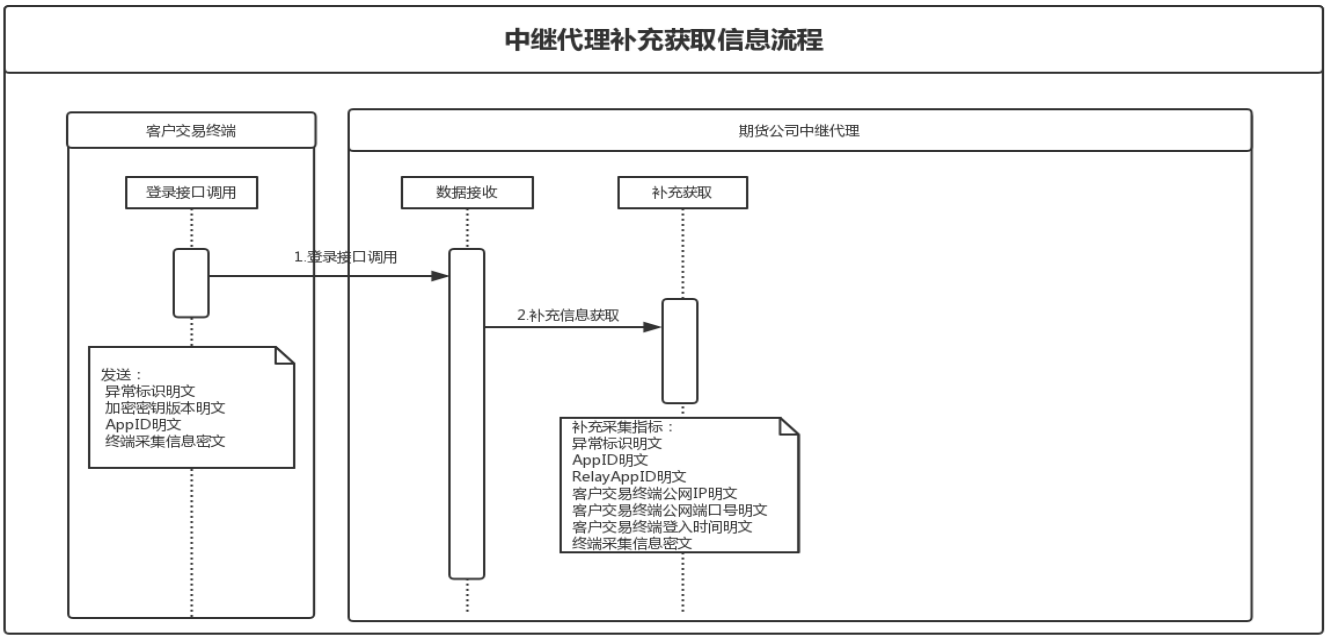
b） 中继模式

1） 客户交易终端



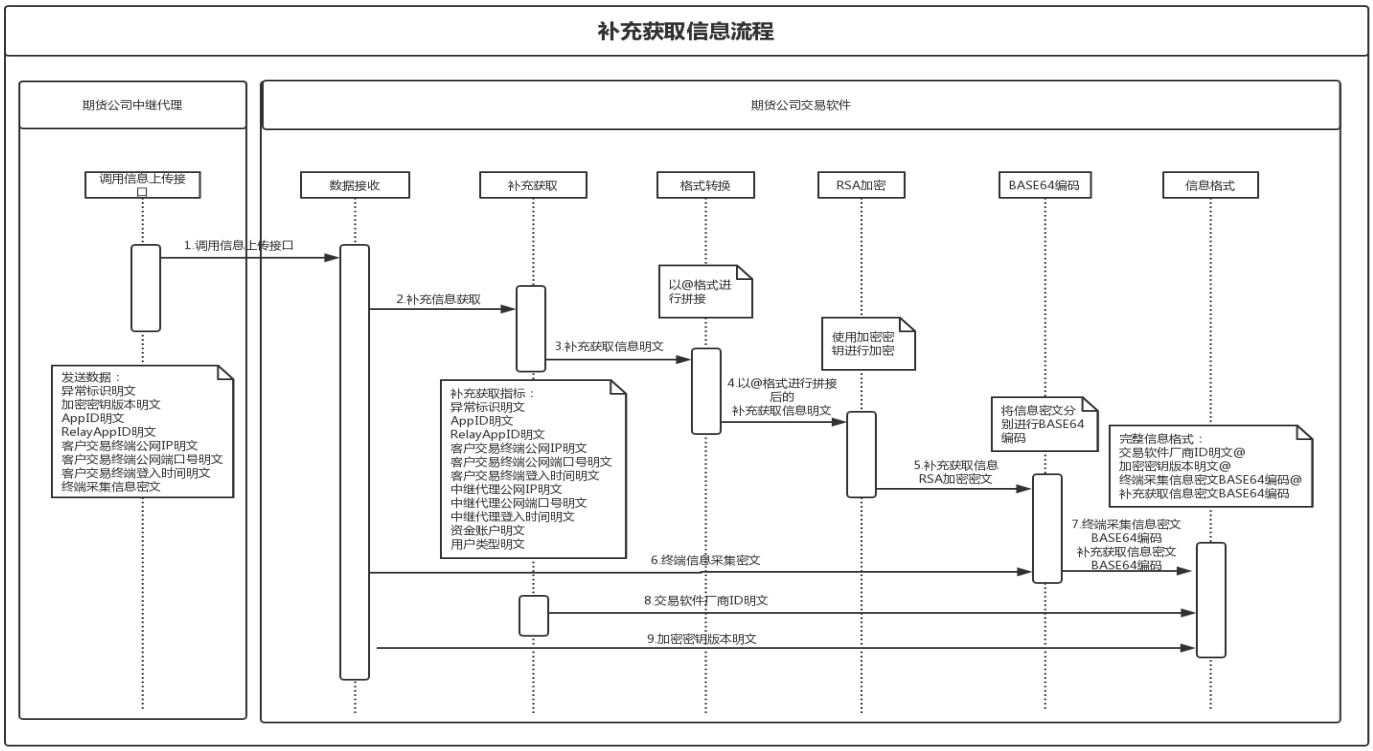
图A-3 客户交易终端信息采集流程

2） 期货公司中继代理



图A-4 期货公司中继代理信息处理流程

3） 期货公司交易软件



图A-5 期货公司交易软件信息处理流程

附 录 B

（参考性附录）

本附录仅供参考，不作为规范要求

B.1 采集流程示例

用户可以直接使用CTP交易API进行交易，也可以通过中继服务器间接调用交易API进行交易。这就需要将信息采集动态链接库和CTP的交易API分离开来，因此信息的采集和上报有可能需要分为两步，API需要增加新的交易API接口（SubmitUserSystemInfo）让用户终端填写上报终端系统信息。

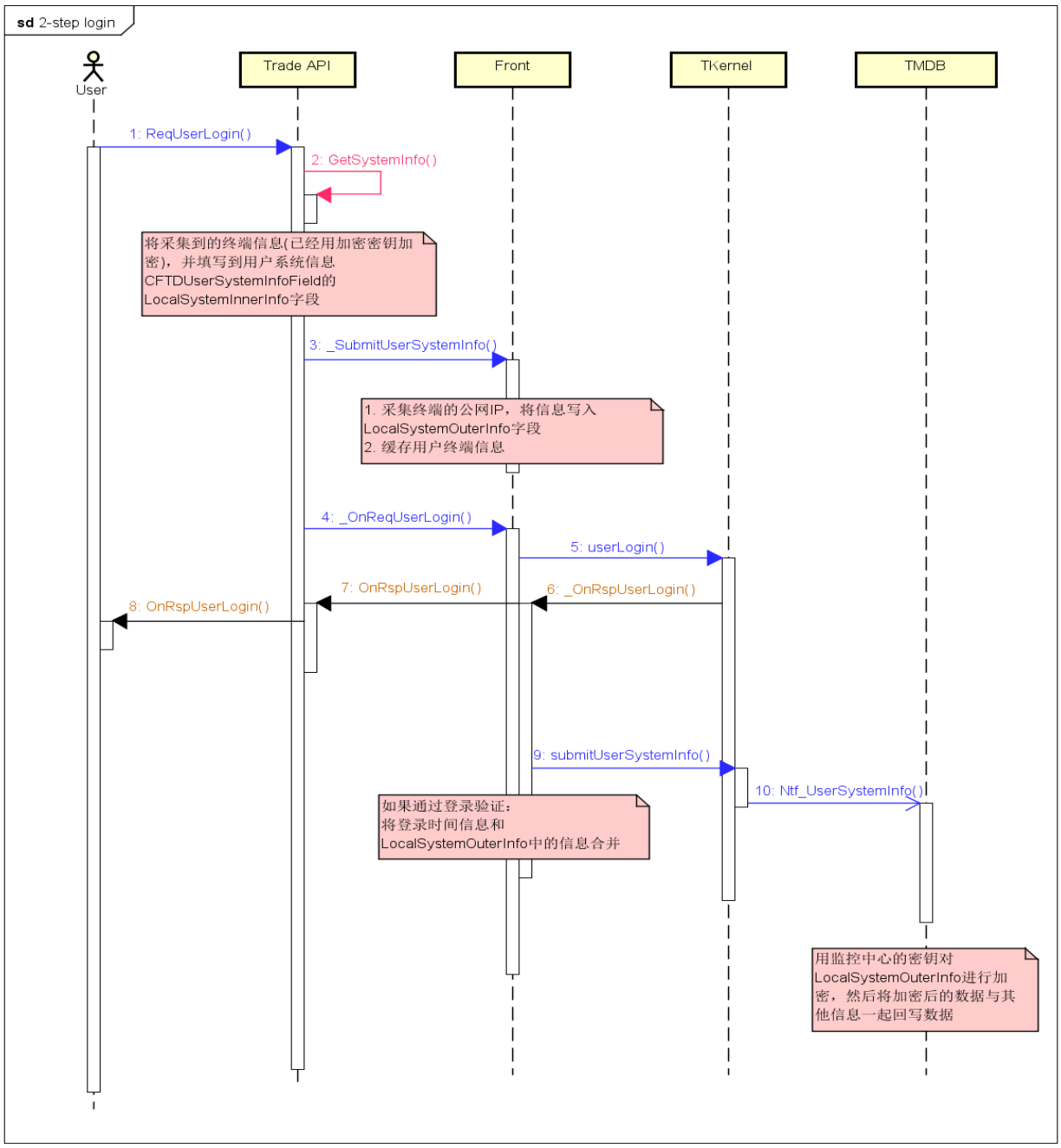
为了保证上报的信息是来自信息动态链接库，CTP在信息采集动态链接库中对已经使用密钥加密的信息进行二次加密。另外，在直接使用CTP交易API进行交易时（直连模式），用户不需要调用SubmitUserSystemInfo交易API接口上报系统信息。如果用户调用了SubmitUserSystemInfo交易API接口，根据登录之前终端认证通过的AppID或者RelayAppID可以区分该终端是直连模式、中继代理模式。对于直连模式调用SubmitUserSystemInfo接口，直接返回失败。在调用登录接口时仍会自动采集本机的终端信息。

a) 直接使用CTP交易API直连模式

直接使用交易API进行交易时，API会直接调用GetSystemInfo()采集终端信息，并将信息填入LocalSystemInnerInfo字段，通过ReqUserLogin()将采集到的信息送给前置。前置收到交易API的ReqUserLogin请求后采集客户端的公网IP，并将该信息填写到登录请求的LocalSystemOuterInfo，然后将登录请求发送给交易核心。

交易核心收到用户登录请求后，验证密码等信息。若通过验证则将请求中的客户端信息发送给TMDB(内存数据回写数据库组件)，TMDB(内存数据回写数据库组件)用监控中心发布的加密密钥对LocalSystemOuterInfo字段的信息进行加密，然后将该信息与其他信息一起回写数据库，结算软件读取数据库，将信息上报给监控中心。

流程如下图:



图B-1 直接使用交易API模式

LocalSystemInnerInfo里面存储的为加密密钥加密后的终端数据。

LocalSystemOuterInfo里面存储的为明文的公网IP和登录时间，入库之前需要用加密密钥加密。

带下划线的函数，为CTP交易系统内部函数。如_SubmitUserSystemInfo。

步骤：

1) 当终端软件通过交易API发起登录请求时，交易API调用GetSystemInfo()采集终端信息，将该信息填写到登录请求的LocalSystemInnerInfo字段中。上报用户系统信息给交易前置。

2) 交易前置收到用户系统信息上报后，采集终端的公网IP填入LocalSystemOuterInfo字段，缓存该用户的系统信息，每个用户只缓存一条信息。

3) 交易API发送登录请求给交易前置。交易前置转发给交易核心。

4) 交易核心验证登录请求，并返回登录响应。

5) 如果交易前置收到成功的登录响应，将响应中的登录时间与LocalSystemOuterInfo合并，通过tresult发送给TMDB。

6) TMDB用监控中心的加密密钥加密LocalSystemOuterInfo信息,然后将所有的用户系统信息回写到物理数据库中。

7) 结算软件读取物理数据库中的信息，每日汇总所有的采集信息，将信息报送给保证金监控中心。

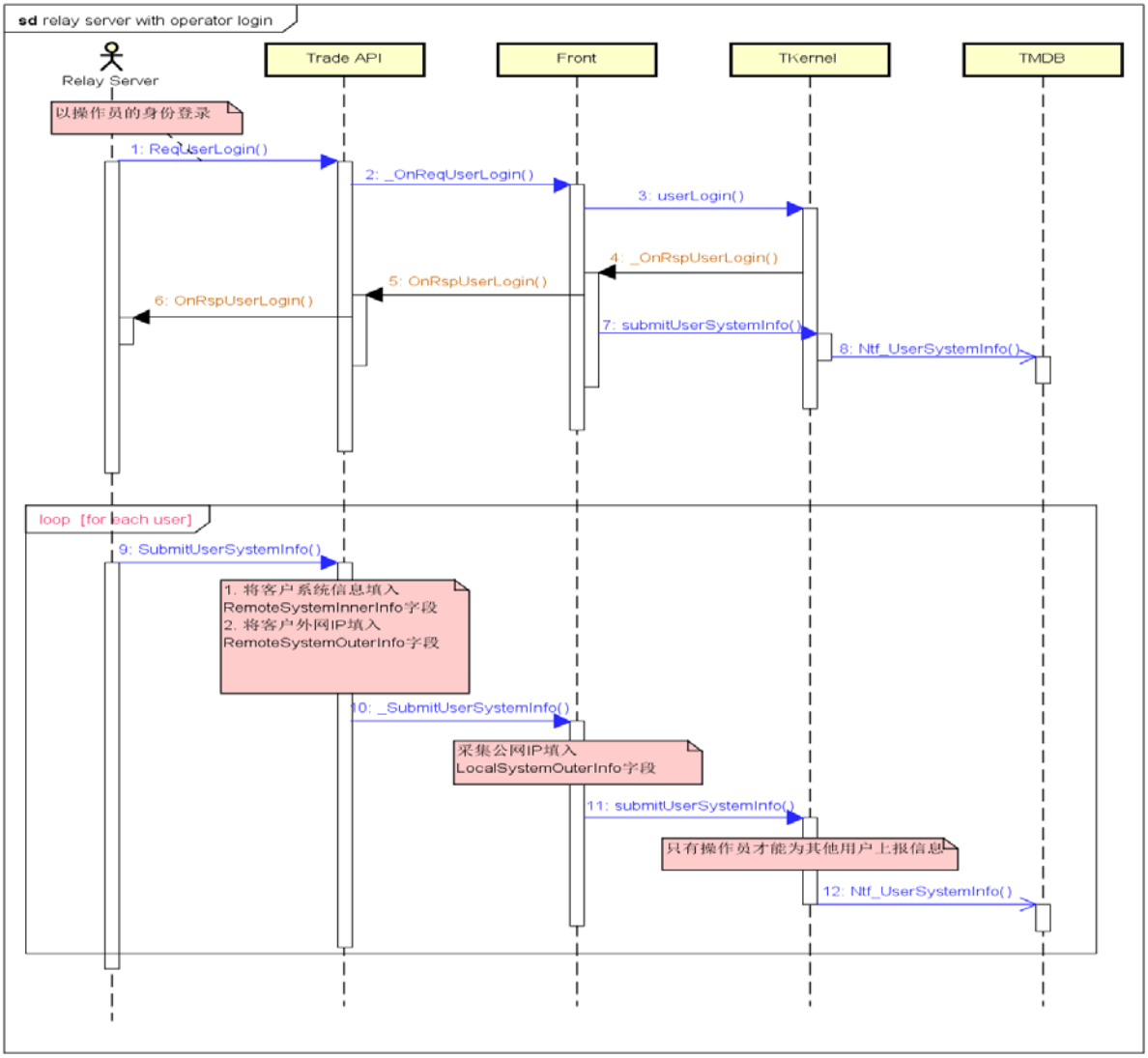
b) 使用中继服务器操作员登录模式

采用中继服务器操作员模式时，信息采集的流程分为两个步骤：

1) 中继服务器以操作员的的身份调用TradeAPI登录CTP交易系统，这时交易后台对信息采集的处理方式同上。

2) 中继服务器成功登录CTP交易系统后，须将客户的终端信息报送上来。

流程如下图所示：

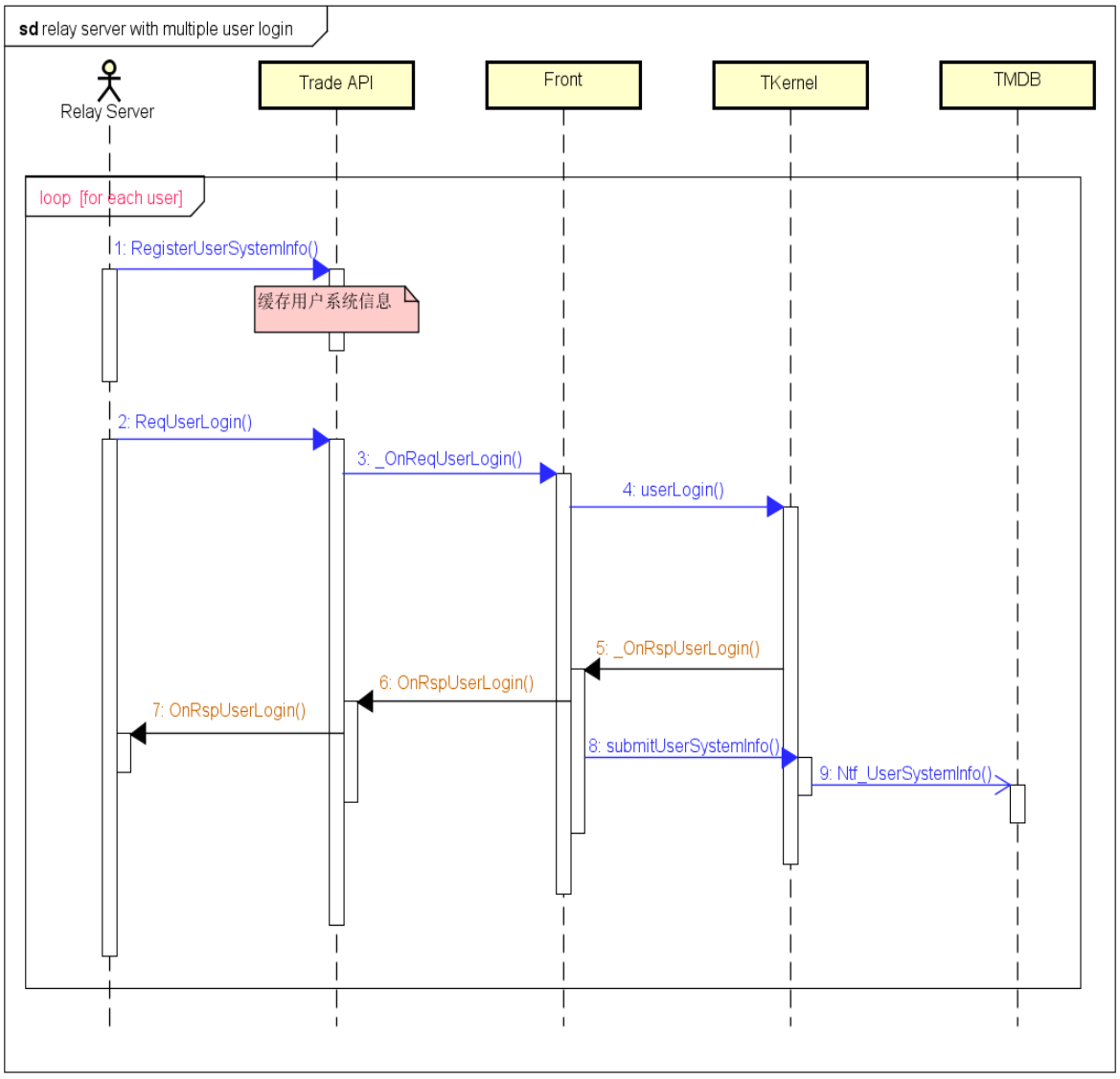


图B-2 中继服务器操作员登录模式

具体步骤：

1) 中继服务器先以操作员的身份调用交易API登录CTP系统，登录时采集信息的方式与用户直接连接时相同。
2) 中继服务器须采集客户端的信息，然后调用SubmitUserSystemInfo()上报终端信息（包含客户终端采集的信息、终端的AppID、终端的登录时间和公网IP、中继服务器的RelayAppID等）。
3) Front采集中继服务器的公网IP，并将信息填入LocalSystemOuterInfo字段中，然后将信息发送给tkernel。
4) tkernel收到数据上报消息时，判断该登录账户是否有数据上报权限（只有操作员和超级用户有为其他用户上报信息的权限）。如果没有权限，直接丢弃消息。如果有权限则将信息发给TMDB。
5) TMDB用监控中心的加密密钥加密LocalSystemOuterIno和RemoteSystemOuterInfo等字段，然后将加密后的信息和采集的终端信息写入物理数据库，结算软件读取该数据库，将信息上报给监控中心。
6) SubmitUserSystemInfo交易API接口只对操作员类型的中继服务器开放使用，其他类型的终端或者中继调用会直接返回失败。

c) 使用中继服务器非操作员模式



图B-3 中继服务器非操作员模式

具体步骤：

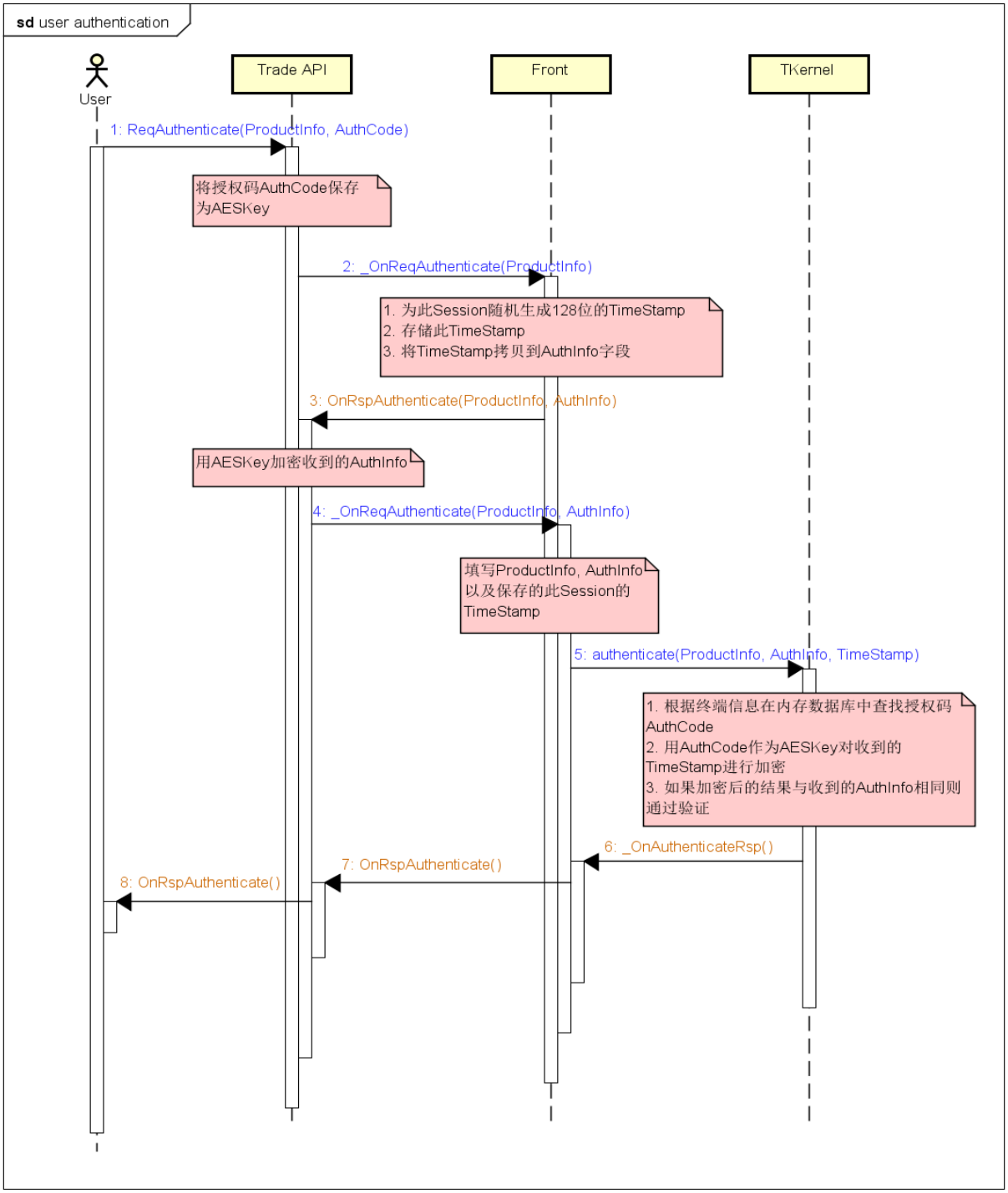
1) 中继服务器先为用户调用交易API的RegisterUserSystemInfo()接口（填写信息包含客户终端采集的信息、终端的AppID、终端的登录时间和公网IP、中继服务器的RelayAppID等）。
2) 其余过程与用户直接连接时相同。
3) RegisterUserSystemInfo交易API接口只对多对多类型的中继服务器开放调用，其他类型的终端或者中继调用会直接返回失败。

B.2 认证流程示例

登录前认证

当客户直接使用CTP交易API时，客户的终端软件（或者中继服务器）必须存有期货公司分配的授权码，在调用ReqAuthenticate()时填入AppID和对应的授权码，交易API将该授权码（暂定16字节）缓存下来作为加密的AES_KEY，以对后续信息进行AES加密。

接入认证的流程如下：



图B-4 认证流程

处理流程：

a) 在终端登录之前，用户通过交易API发起终端认证请求ReqAuthenticate。需要用户填写AppID（RelayAppID）和授权码（authcode）， 该授权码只会缓存交易API中，不会在网络中直接传输授权码。
b) 交易前置随机生成128字节的TimeStamp，将TimeStamp保存在session信息中 ，并将其通过RspAuthenticate回调信息返回给终端。
c) 终端收到RspAuthenticate回调信息后，使用AES_KEY加密TimeStamp，并将其赋值到AuthInfo字段，再次发起ReqAuthenticate请求
d) 交易前置收到第二次的FTD_TID_ReqAuthenticate之后，将之前session保存的TimeStamp 赋值到请求里面的TimeStamp字段中。将认证消息发送给交易核心
e) 交易核心使用内存数据库中终端信息对应的授权码加密TimeStamp字段，并将加密结果与AuthInfo比较。如果相同设置当前终端为已经认证。并返回RspAuthenticate成功结果给交易前置。
f) 交易前置通过API回调，将认证结果返回给用户
g) 对于认证失败的连接，不允许进行登录。

B.3 信息采集函数参考

PC终端（Windows）	信息采集时间	time();
	私网IP	gethostname()和gethostbyname();
	公网IP	gethostbyname()和inet_ntoa();
	网卡MAC地址	getAdaptersInfo();
	硬盘序列号	1.CreateFile()和DeviceIoControl(); 2.system("wmic path win32_physicalmedia get SerialNumber");
	操作系统版本	GetVersionEx()、VerifyVersionInfo()和NetWkstaGetInfo();
	设备名	GetComputerName();
	CPU序列号	使用System命令wmic CPU get ProcessorID;
	系统盘分区信息	1.GetLogicalDriveStrings();GetDriveType();GetSystemDirectory 2.使用System命令 Diskpart list volume;
	BIOS序列号	wmic bios get serialnumber
PC终端（Linux）	信息采集时间	time();
	私网IP	ioctl();
	公网IP	gethostbyname()和inet_ntoa();
	网卡MAC地址	ioctl();
	硬盘序列号	1.通过hdparm命令或者lshw命令; 2.使用ioctl(fd, HDIO_GET_IDENTITY, id2)方式获取; 3.scsi_io(fd, cdb, sizeof(cdb), SG_DXFER_FROM_DEV, data, &data_size, sense, &sense_len);
	操作系统版本	uname();

	设备名	1.使用hostname shell命令; 2.gethostname();
	CPU序列号	1.linux：使用<cpuid.h>的__get_cpuid(level, &eax, &ebx, &ecx, &edx); 2.dmidecode -t 4 | grep ID;
	BIOS序列号	dmidecode -t 1|grep "Serial Number"
PC终端（Mac OS）	**信息采集时间**	time();
	私网IP	NSHost*myhost= [NSHostcurrentHost(私有api)]和NSString*ad = [myhost address];
	公网IP	gethostbyname()和inet_ntoa();
	网卡MAC地址	GetPrimaryMACaddress();
	硬盘序列号	IOKit framework;
	设备序列号	IOKit framework;
	操作系统版本	Long response=Gestalt(gestaltSystemVersion,&response);
	设备名	IOKit framework;
移动终端（Android）	**信息采集时间**	1.Calendar.getInstance().getTime(); 2.System.currentTimeMillis;
	公网IP	HttpURLConnection;
	移动终端IP	1.NetworkInterface.getNetworkInterfaces(); 2.getSystemService(Context.WIFI_SERVICE).getConnectionInfo().getIpAddress()||NetworkInterface.getNetworkInterfaces().getHostAddress().toString();
	手机号码	1.TelephonyManager.getLine1Number() 2.TelephonyManager tm =(TelephonyManager) this.getSystemService(Context.TELEPHONY_SERVICE)tm.getLine1Number();

	移动设备唯一识别码（IMEI，MEID）	1.TelephonyManager.getSimSerialNumber(); 2.tm.getDeviceId();
	地理位置信息	LocationManager, Geocoder;
	操作系统版本	1.android.os.Build.VERSION.SDK_INT; 2.PackageManager()/UIDevicecurrentDevice;
	设备序列号	1.android.os.Build.SERIAL; 2.Secure.getString(getContentResolver(),Secure.ANDROID_ID);
	设备MAC地址	1.NetworkInterface.getNetworkInterfaces(); 2.NetworkInterface.getByInetAddress(InetAddress.getByName(getLocalIpAddress())).getHardwareAddress();
	设备名	android.os.Build.DEVICE;
	设备类型	android.os.Build.TYPE;
	IMSI	String imsi =telManager.getSubscriberId();
	ICCID	Android:String iccid =tm.getSimSerialNumber();
移动终端（iOS）	信息采集时间	[NSDate date];
	移动终端IP	1.getifaddrs(); 2.系统方法获取sys/socket.h;
	通用唯一识别码（UUID）	可能需要第三方库来保存信息 或[uuid转化 imei]/UIDevicecurrentDevice;
	地理位置信息	CLLocationManager;
	操作系统版本	systemVersion或PackageManager();

	设备序列号	[UIDevicecurrentDevice]获取;
	设备名	struct utsname systemInfo; uname(&systemInfo); NSString *deviceName = [NSString stringWithCString:systemInfo.machine encoding:NSUTF8StringEncoding];
	网络运营商	CTTelephonyNetworkInfo *info = [[CTTelephonyNetworkInfo alloc] init]; CTCarrier *carrier = [info subscriberCellularProvider]; mobile = [carrier carrierName];
	设备类型	NSString *deviceType = [UIDevice currentDevice].model;
其他终端（微信委托）	**信息采集时间**	系统接口
	OpenID	WxOpenIdServlet 微信公众号开发网页授权获得OPENID
	地理位置信息	使用微信公众号JS-SDK提供相应接口
其他终端（线下委托）	**信息采集时间**	系统接口
	电话号码	服务器端采集