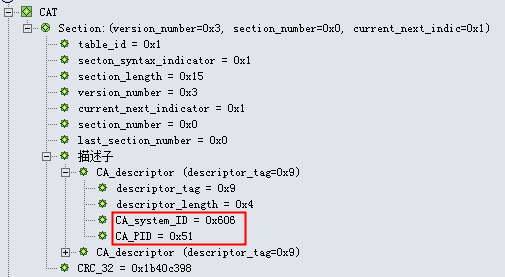
## CA解扰流程

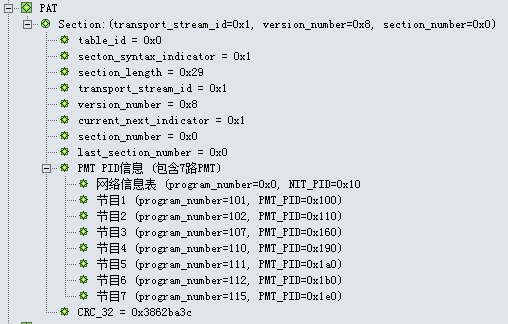
1. CA系统结构简介
2. 集成管理系统（IMS）：设置参数，连接、控制、管理系统；
3. 节目管理系统（PMS）：对节目定义、编辑、编排、查询、节目时间表的产生；
4. 用户管理系统（SMS）：用户信息、用户设备、节目预定信息、用户授权信息、财务信息的维护管理，并提供给其他子系统进行查询；
5. 前端条件接收系统（CAS）：对用户授权控制信息（ECM）和用户授权管理信息（EMM）信息的获取、生成、加密、发送等；
6. 电子节目指南系统（EPG）：提取节目数据库中的节目描述信息，转化为SI信息，按照一定的周期发送给复用器；
7. 复用加扰系统（MSS）：定义同密同步器（SCS）、授权管理信息发生器（EMMG）、业务信息发生器（SIG）接口，采用标准DVB加扰算法；
8. 条件接收端CA系统：接收前端发来的EMM、ECM数据，并与智能卡进行交互，获取解扰控制字，让解扰器完成解扰工作。也会提供CAS辅助信息给接收设备，用于必要信息的显示；
9. 智能卡发行系统：发行各种智能卡，如系统母卡、系统钥匙卡、用户接受卡等，其都是用不同的发行系统完成的
10. 终端CA相关基础知识介绍
11. CAT表结构



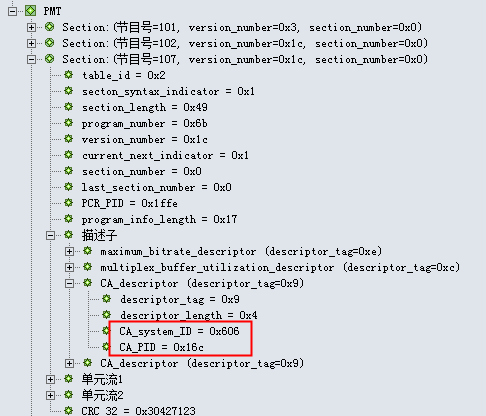
**CA\_system\_ID**: 是码流的加密方式的标识，区别各种CA；

**CA\_PID**:EMM数据包的PID

1. PAT表分析



1. PMT表分析



**CA\_system\_ID**：是码流的加密方式的标识，区别各种CA；

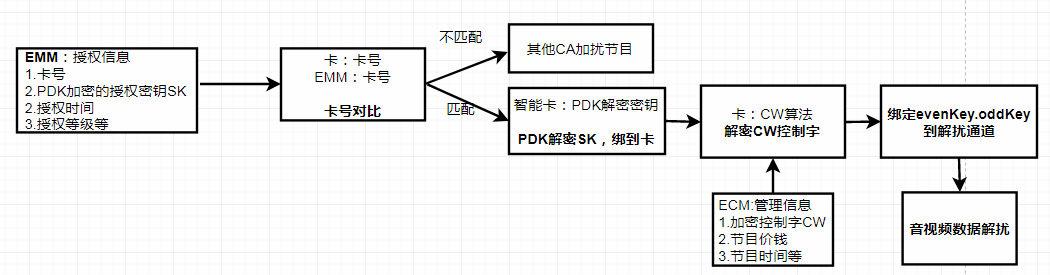
**CA\_PID**：ECM数据PID

1. 常见的CA厂商

|  |  |
| --- | --- |
| **常见厂商ECM数据标识** | |
| 国内 | 国外 |
| 同方: 0x4a02 和 0x49xx | Viaccess: 0x0500 to 0x05FF |
| 数码视讯: 0x4ad2 | Irdeto: 0x0600 to 0x06FF |
| 天柏: 0x4a30 | NDS: 0x0900 to 0x09FF |
| 算通: 0x3000 和 0x4abx | Conax: 0x0B00 to 0x0BFF |
| 数字太和：0x4aed | NagraVision:0x1800 to 0x18FF |
| 锋尚: 0x66 |  |
| Irdeto： 0x06 |  |

SDT表→PAT表（一直在进行请求）→PMT表→找到所需节目的TS包→CAT表→解扰→解码

1. 解扰（以下以Irdeto为例）
2. 解扰基础原理

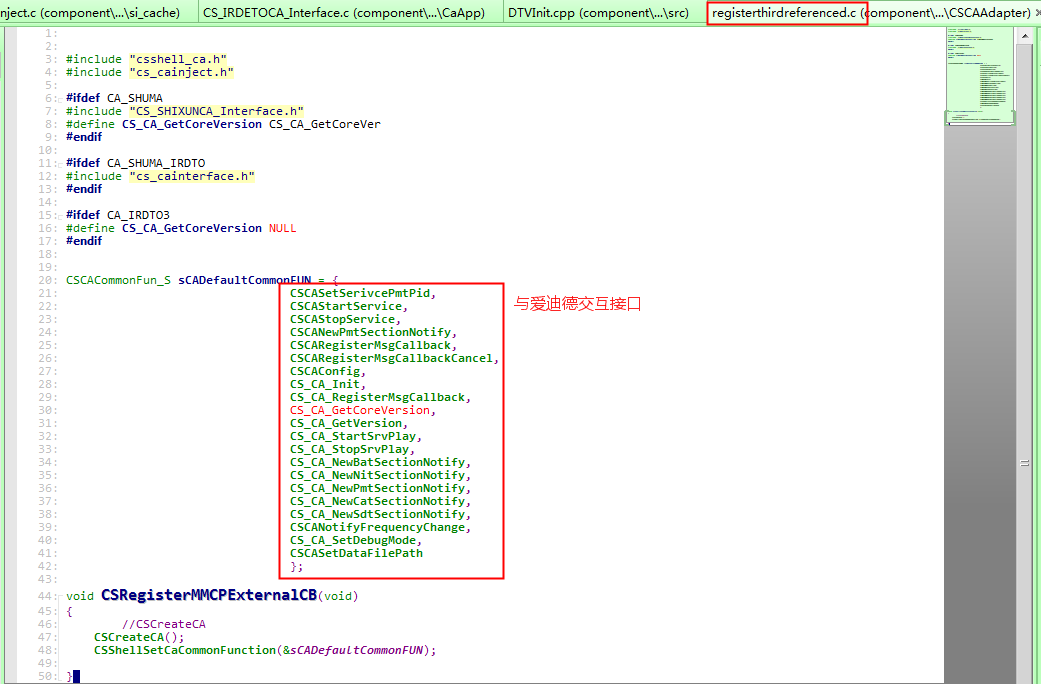


图表 1终端CA解扰原理图

解扰步骤：

1. CAT表中获得EMM数据；
2. 获得EMM数据中的卡号信息；
3. 卡号信息的对比，判断是否有权观看该节目；
4. 卡号不匹配，不是该卡/用户的授权节目；
5. 卡号匹配，使用智能卡中有用户PDK私密密钥（PDK公密在信号发送系统中，对信号进行加密），解密EMM数据中的SK加密数据，再将SK绑定到卡上；
6. 获取ECM信息，包含加密的控制字CW；使用SK对CW进行解密；
7. 将CW随机码绑定到解扰器，对数据进行解扰；
8. 再进行解复用，解码，得到原始的音视频数据进行播放；
9. 解扰流程
10. CA服务的创建
11. CA服务的启动

CA服务启动的几种情况：



CA的创建--- CSCreateCA();

CA启动：



数据的要求：

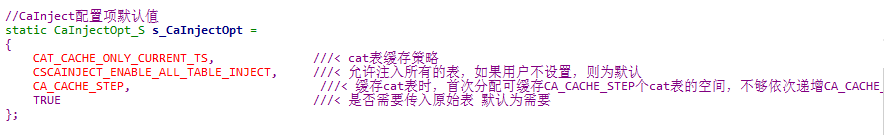
CSSICLoadTable()🡪SI\_CaChe模块给出表的数据

SI\_CaChe：将表数据进行缓存，等待其他模块的查询

Section:数据的过滤和缓存，底层数据的过滤管理，以及数据包PID冲突的处理

开启CA的设置：

1. 是否需要传入原始表（加扰方式处理/清流方式处理）；
2. DemuxID、ServiceID、OriID、TsID、音视频ID、CA厂商ID、emmID、ecmID



CA启动的原因：

CA启动调用---》CSCATCallback；CSPMTCallback

1. 频点的变化；
2. 节目基本信息未变，但是音视频数据引起的变化（CAT不会再次注入）；
3. 同一个频点之间的切台；
4. PMT与DM保存的PMT表信息发生了变化；
5. 需要记录的信息：demuxID、tsID、origintsID、serviceID、audioID、vedioID、视频播放、CSOnCaCtrlWordCome\_FCW（用于CW数据回传给应用）、
6. 关于PMT信息的设置：将PMT中的相关信息设置，用于后续对音视频数据的获取；m\_fnCSCASetSerivcePmtPid
7. 启动播放/录制；m\_fnCSCAStartService
8. 将CAT数据传给CA模块；m\_fnCS\_CA\_NewCatSectionNotify

CSCASetSerivcePmtPid

m\_fnCSCAStartService

m\_fnCS\_CA\_NewCatSectionNotify

m\_fnCSCANewPmtSectionNotify

由DTV通知到CaApp模块：

CaApp(CAT/PMT数据变化通知、NIT数据变化通知)



CaApp发送信息：

11.DisposeMsgToFta本模块之间传递信息

22.Task调用CS\_CA\_DirectMessage接口，将数据传到CaApp模块，调用CAProductCheck

接口对数据进行处理，

SOLTimerProc这个是卡校验的检查，若校验发现卡状态是错误的，将向CaApp上报错误信息。

SOLDisposeSvcValidation校验函数

SOLComposeRSASrcData被BAT和NIT调用

1. CAGetSOLFlag判断，SOLRequestPatTask检测PAT表，

CA初始化是，开启了计数器，进行开始或者停止播放是，计数器停止。开始播放，是因为2个表收集全了；

再问：这两个表是什么，是PMT和CAT还是CAT和PAT。

再答：

1. CAGetFtaBlockFlag判断

Task对UI接口进行了注册，CS\_CA\_UIQuery –》 数据到来 --》 CA\_UiReplytMail –》DisposeMsgToFta –》调用DTV的回调函数，向DTV返回消息（单个节目菜单信息中的ECM/EMM节目信息）

CaTask接收到消息，CA\_TASK\_SendMessage（厂商通过该接口向CAtask发送信息）

CaTask：CaTaskMain数据接口---》CaProcessMsg处理消息接收来自外界模块的所有信息（其中包括emm、数据、ecm数据、以及nit中的信息、卡的消息处理）

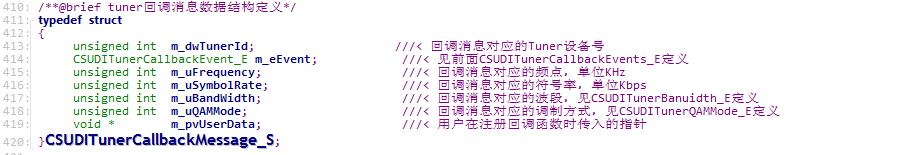
TASK 模块通过CaProcessMsg接口只解析两种数据：

1. CADRV\_\_SCELL\_MESSAGE：来自softcell的数据，CA库；
2. CADRV\_\_CA\_TASK\_MESSAGE ：其他模块向CA传递的数据，经过解析之后，与与CA库进行交互；

sic\_loader\_monitor(),一直在data\_receiver接收数据；sic\_parseTable解析各种表，

与tuner的检测变化：

频点、符号率、调试方式、锁频是否成功、带宽；



DTV模块数据通知：

CS\_CA\_NewCatSectionNotify

CSCANewPmtSectionNotify

；

数据解析模块：

CA本地接收到数据信息之后，对数据进行分析的接口：afnParseReply处理函数 --- ProcessSCellMsg --- IA\_WriteToMessage向库里写数据；

IA\_ReadFromMessage向库中读取数据 – 用户向CA请求信息或者通知CA进行动作：afnQueryControl --- CA\_TASK\_QueryControl

回调注册用户（CaApp）接口，为了CaTask回发消息；

CaApp接收到消息之后，调用DisposeMsgToFta接口，将消息给DTV的回调函数，进行消息的处理，如，其他CA节目

其中CA\_DRV\_Message接口只是传递了消息，task并不处理消息；

1．CS\_CA\_DirectMessage接口是UI接口的回调，CA会向上层应用抛消息。CS\_CA\_UIQuery对信息进行处理；

2.iIrdCACallBack接口是DTV的回调，CA通过这个接口向DTV中的插件抛消息，iIrdCACallBack对接收到来自CA的信息进行处理；

1. EventStatusCallBack是CA向智能卡注册的回调，当卡转台变化的时候，通知CA；

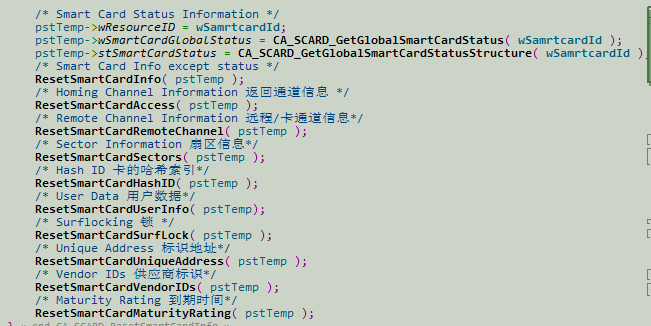
3.DTV其他模块的回调，

EMM数据传到CA库中：CA\_SVCINFO\_EmmSvcNotify—》CA\_NOTIFICATION 回调函数（通知）

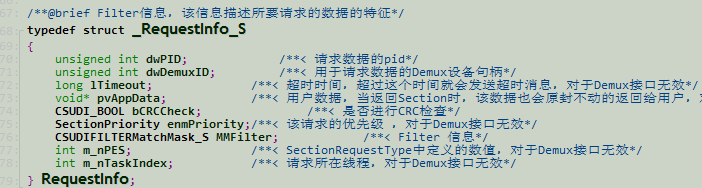
解扰服务相关：

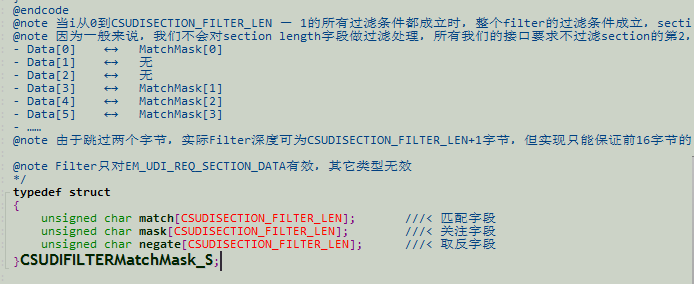


卡信息：

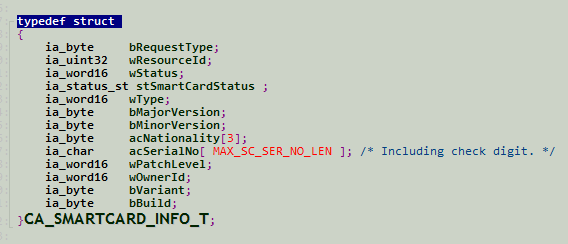


1. CSUDISMCDataExchange进行卡信息的交互
2. 设置通道PID，过来数据包。设置过滤器的





本地存储关于卡的信息，为响应本地请求，用户信息的查询，CA\_TASK\_QueryControl接口用于被用户调用查询CA数据或者通知CA进行什么动作：



1. 问题思考
2. 如何判断是该用户的节目，还是其他用户的节目？

在解密得到的EMM数据信息中有卡号信息，与我们从智能卡中获取到的卡号进行对比，校验不成功，便说明不是该用户的节目；若校验成功了，便将EMM、ECM数据传送到智能卡中，获得CW值返回机顶盒，绑定到解扰通道，进行数据的解扰播放。

1. 如何判断DVB码流是加扰码流的？

PMT数据中，有ECM字段，便说明是加扰的；

IrdetoCaTaskMain在caapp中，实时的对cat和pmt进行监测。这两个表的监测是有DTV进行实时的通知的。

CA\_ParsePmtChanged接口对PMT数据进行了分析，依据描述符信息判断是否加扰节目。

SOLChangeCurrentSvcFTAFlg();告知，是否是清流（清流有区分），还是加扰流。若是加扰流，

11.进行SOLCheckSignatureByRSA（）校验，

CA\_RSA\_Verify（），用pcPublicKey 对pcData的签名值进行校验，

数据：

1、CS\_CA\_SOLParseBATData（），在BAT描述符中，前端md5+RSA后的加密数据；

2、SOLComposeRSASrcData（），在BAT数据正取的前提下，在NIT表数据中提取描述符，得到SRC原始数据，在0x95描述符中的tsdata 和0x95的描述符

3. CA\_RSA\_Verify（），用pcPublicKey 对pcData的签名值进行校验，使用信息摘要算法MD5；

4. CA\_RSA\_Decrypt（）；进行解密，RSA\_RsaDo（）；检验返回

22.向CaApp发出通知，（频点变化就等待获得PAT表，未变化且没有错误就上报），CaAPP会继续想DTV模块进行通报。

1. 音视频数据是如何被实时解扰的？

CW伪随机码被绑定到指定的通道中，对数据实时的解扰；

1. EMM、ECM数据是如何向其他的APP转发的？

获得EMM和ECM数据之后，传递至CaTask进行解析；

DefineDescrambleService（）；CA\_CLIENT\_DESCRAMBLE\_SERVICE\_TYPE卡翻新

DefineDMBDescrambleServices（）；CA\_CLIENT\_DMB\_DESCRAMBLE\_SERVICE\_TYPE

1. Videoid、audioid、emmid、ecmid、streampath参数哪里得到的？

在创建CA的时候，也创建了这些信息的结构体，接着在开启CA服务的时候，应用已经传递了这些基础信息；

再问：那么应用是如何拿到这些消息的呢？

再解：从DTV模块查询的得到的

1. CA还做了什么事情？

版本信息查询、chipID、授权状态查询、OSD显示、指纹显示等

1. CA需要提供的接口有哪些？

解扰操作接口：接收解扰通知信息，如被DVBPlayer调用

CA应用接口：APP直接的交互

1. CAT、PMT数据为什么要同时获取，他们之间又是如何控制获取的？

并不是说必须同时获取，只是都是解扰所需要的，那就一起获取了。

他们之间的配合，有共同的CA\_ID值，保证是同一个CA厂商的。

1. 应用是如何实现音视频的播放的，为什么还会有应用传递过来的CA通知？

DVBPlayer通知开始解扰，接着就是中间件启动解扰，获取数据进行解扰。

1. PIN是如何被使用的？
2. 伪随机码的概念？

用于加扰的数据，与原始音视频数据进行异或运算，得到加扰码流；

用于解扰的CW值，在与码流数据进行异或运算，解扰，得到音视频原始流；

1. 控制字的作用是什么？

即初始值，控制随机码发生器的初始化；

1. CA控制端与CA客户端，是如何配合工作的？

加扰端与未加扰端的伪随机码发生器是相同，伪随机码发生器的起始点（初始化）相同，所产生的随机码就是相同的，实现匹配，进而解扰。

1. EMM（授权信息）数据的形成

用户卡中的密钥（Key）解密授权密钥（PK），其中包括卡号、授权时间、授权等级等用户管理信息；

1. ECM（管理信息）数据的形成

授权密钥（PK）对ECM进行解密，得到控制字（CW），其中包含时间、节目价钱、节目授权控制等；

1. 明文控制字与密文控制字如何得到的，拿到之后我们有做处理吗，他们之间区别是什么？

由CA库进行解密运算得到（CA厂商来做的）；

我们拿到之后，可以处理也可以处理，处理就进行和校验，实质就是进行数据长度的判断；

奇偶校验值的区别：不同的平台有不同的处理方式，密文直接绑定到通道；

再问：奇偶校验值，是如何被使用的？

再答：SK被保存在智能卡中，但是CW需要不断的更新（ECM数据的不断更新），为需要解决新旧密钥的替换问题，为下次激活做准备。

1. EMM数据是如何获取授权的，或者说是如何控制用户的使用时长的？
2. System\_id所影响的是什么，这个与密钥索引是不是一个东西？

影响到了CA系统厂商为机顶盒厂家分配密钥组；

再问：密钥组的作用是什么？

再答：密钥组是在进行CW控制字运算的时候，需要使用到的。

1. 加密的CW控制字是谁负责计算的，在哪里计算的？

由密钥组和加密的ECM数据信息结合CW算法得到的。

CW是由SK进行加密的，SK是需要不断的进行更新的。

SK又被PDK个人密钥加密，生成了EMM数据。

PDK私密是被放置到智能卡中进行解密，PDK公密在信号发送系统，用于对信号进行加密，这个过程也叫数字签名的认证过程。

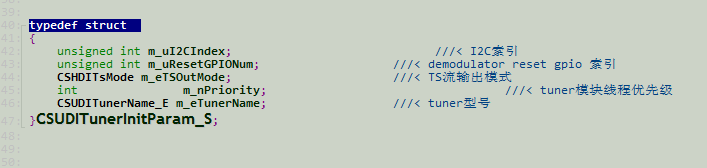
1. 解扰与高安设置之间的关系？

高安的要加设CWPK值

表更新的通知

1. 初始化，进行监测，tuner准备OK便可以开始取数据；
2. 如何频点的变化；

Tuner初始化：



Tuner状态监测：

由RDITunerDetectDevice（）实时监测；

CAmanager与DTV插件实时的进行交互，如，获取邮件数量，删除邮件等

DTV插件，进行相应动作（向CA模块查询相应的信息，并返回）；

DTVmanager与DTVadapter进行交互，到DTV的各模块等进行信息的查询；

解扰启动-流程：

1. BpDTVALManager::DTVAL\_caStartDescrambling（DTV客户端接收到DVBPlayer通知）
2. BnDTVALManager::onTransact 🡪DTVAL\_DTVAL\_caStartDescrambling（DTV服务端接收）

调用：reply->writeInt32(DTVAL\_caStartDescrambling(&stDesCrambleParam))

CSNotifyStartCA（）通知到cache模块

1. CaInjectTaskMain（）进入到实时监控来自应用开始解扰的通知
2. 进行CSStopCA（）

iLocalRequestPAT（）

iLocalRequestCAT()

CSStartCA()

VD\_IO:

CS\_VD\_DF\_IO 过滤器的设置

DMUX\_DRV\_SetChannelPid

DMUX\_DRV\_AllocateFilter

DMUX\_DRV\_SetFilter

DMUX\_DRV\_GetSection

CS\_VD\_SC\_IO智能卡交互

CS\_VD\_DD\_IO解扰

CSDSMAllocateDescrambleEX

VD\_DD\_SET\_PID：CSDSMSetDescramblePID设置需要解扰的数据PID

VD\_DD\_SET\_KEY：CS\_CA\_ProcessCW

CSDSMDescrambleSetOddKeyValue

CSDSMDescrambleSetEvenKeyValue

VD\_DD\_SET\_SKEY：高安设置的

CS\_VD\_Loader\_IO OTA升级等

CS\_VD\_PS\_IO NVRAM存储区

CS\_VD\_TIMER\_IO 开启定时器

IRD\_MSG\_ParseDecoderMsg softcell发送的信息，进行解析，解析好之后，再转发给DTV模块，进行显示等