一般CA加解扰流程

DVB标准的CAS使用同密加密，即不同的CA厂商定义各自的ECM/EMM规则，但是使用相同CW和算法对TS流进行加解扰。

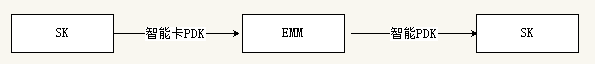
前端使用CW对清流进行加扰，终端使用CW对加据流进行解扰，CW通过ECM、EMM由前端发往终端



前端使用SK加密CW加上节目订购周期、价格、授权控制等信息得到ECM、ECM一般更新较快、加密算法简单、运算快。



前端使用智能卡PDK加密SK加上智能卡识别号、授权起始信息、授权控制信息等得到EMM。EMM更新频率较低、使用更安全的加密算法、运算较慢。



高安芯片加解扰

因为一般CA解扰存在CW泄露的可能，所以使用高安芯片在智能卡解扰出CW后、再二次加密CW，把二次加密的CW发送给高安芯片进行解密，然后直接把解密后的CW用于解扰。高安芯片与主CPU是物理隔绝的，所以主CPU无法获取明文的CW。

智能卡对CW采取层级加密的形式SCK->K1->K2->CW得到密文的K1、K2、CW。高安芯片再采取层次解密的形式SCK->K2->K1->CW得到明文CW。PCK每个芯片唯一在生产时烧录到OTP安全区域。

CW->Control Word

SK->Service Key

PDK->person distributed key

高安芯片原理图：

