# 面向三网融合的视频内容责任认定机制

## 主要业务流程

1. 参与主体：CP（内容提供商），AP（审核部门），NO（网络运营商），USER（用户），都是半诚实参与者。
2. 系统数据流图



图1系统数据流图(cp和ap也有数据交换)

1. 前提条件

参与主体都建立相应的数据库，协商好相应的公钥加密算法和相互公开公钥，保持私钥。

1. 主要业务流程描述

A、送审

1. CP登录AP端；

注：CP通过用户名，密码（cp端发送密码的hash值）登录，这样就可以和AP进行通信了。

1. CP发送请求，AP返回会话密钥TID,，是本次通信的安全标识，防止冒充者；

注：为了安全起见，他们二者之间通过diff-hemma协商一个会话密钥TID，只有二者知道，每次完成一次通信都要先验证此通信TID，防止恶意冒充者攻击。

1. CP选择A、B两组参数对媒体m进行采样，比特承诺，HAm,HBm；

注：A组用于发送验证，保证传输的安全；B组用于对AP返回的媒体进行再次检验，防止AP端的篡改。

1. CP使用AP的公钥pkap加密(TID,A),使用skcp加密HAm(签名)；

注：使用公钥加密（TID,A），AP收到后可以用自己的私钥进行解密，这样整个通信过程没有人可以知道(TID,A)；使用skcp加密HAm得HAmcp(标识为CP私钥加密的结果)，AP可以使用公钥进行解开，获得HAm的值，但是AP无法伪造签名的HAmcp

1. AP解密消息，验证TID，验证HAm，返回验证结果；

如果验证TID失败，就可以终止本次通信，说明不是CP在通信；如果验证成功则继续，进一步验证视频有没有被篡改，如果篡改返回篡改的位置信息。需要设置个消息，用于标识各种错误。

1. AP对视频m进行审核，审核通过后，记录数据库，采样C，返回。

注：对视频内容进行人工或者是机器审核，对于没有问题的视频，则进行记录数据库，并选择C组参数对媒体进行采样，发送公钥加密（TID,C）和私钥加密HCm给CP。

1. CP进行确认，确认C组参数比特承诺的正常，确定B组采样参数的正常，证明AP没有进行内容的更改。

注：在CP端的验证，有TID的验证，有C组的验证，有B组的验证。验证完成，返回一个成功标识。

B、分发运营

1. NO登录CP端

注：运营的时候，NO需要连接CP，获取媒体内容。

1. NO发出请求，CP返回会话密钥TID，是本次通信的标识。

注：CP和NO协商一个会话密钥TID

1. CP使用NO的公钥pkno加密(TID,A),使用skcp加密HAm(签名)；

注：采用审核的通信模式进行通信。

1. NO解密消息，验证TID,HAm，返回验证结果；
2. 如果成功接收，则可以运营，向用户分发视频内容。

C、责任认定

当在网络中发现非法视频传播，需要查找源头时，就需要进行保密比较。

假设：CP所做的签名为HAm\_cp，AP所拥有的签名是：HAm\_ap，同时NO拥有的签名是HAm\_no,USER计算的结果是HAm\_user。如果没有问题，这三者应该是相同的。

1. 首先验证，HAm\_ap，HAm\_no是否是有CP的签名。
2. 进一步验证责任方

情况一：HAm\_ap≠HAm\_no，且HAm\_ap=HAm\_cp，则CP在审核后进行了内容的替换；

情况二：HAm\_ap≠HAm\_user，且HAm\_ap=HAm\_cp，HAm\_cp=HAm\_no，则NO在分发时对内容进行了篡改。

## 数据库设计

### CP端：

AP、NO的公钥信息；CP的私钥信息；媒体数据（媒体名称、CPID、Ham（签名）,HBm,HCm,A，B，C）;NO(NOid,用户名、密码的hash值，公钥路径);

### AP端：

媒体数据（媒体名称、CPID,HAm,A）;

CP表（名称、密码、公钥路径、CPID）;

NO表（用户名、密码、NOID，公钥路径）;

### NO端

媒体数据（媒体名称、CPID,HAm,A）