### 签名正确性分析

* 功能描述

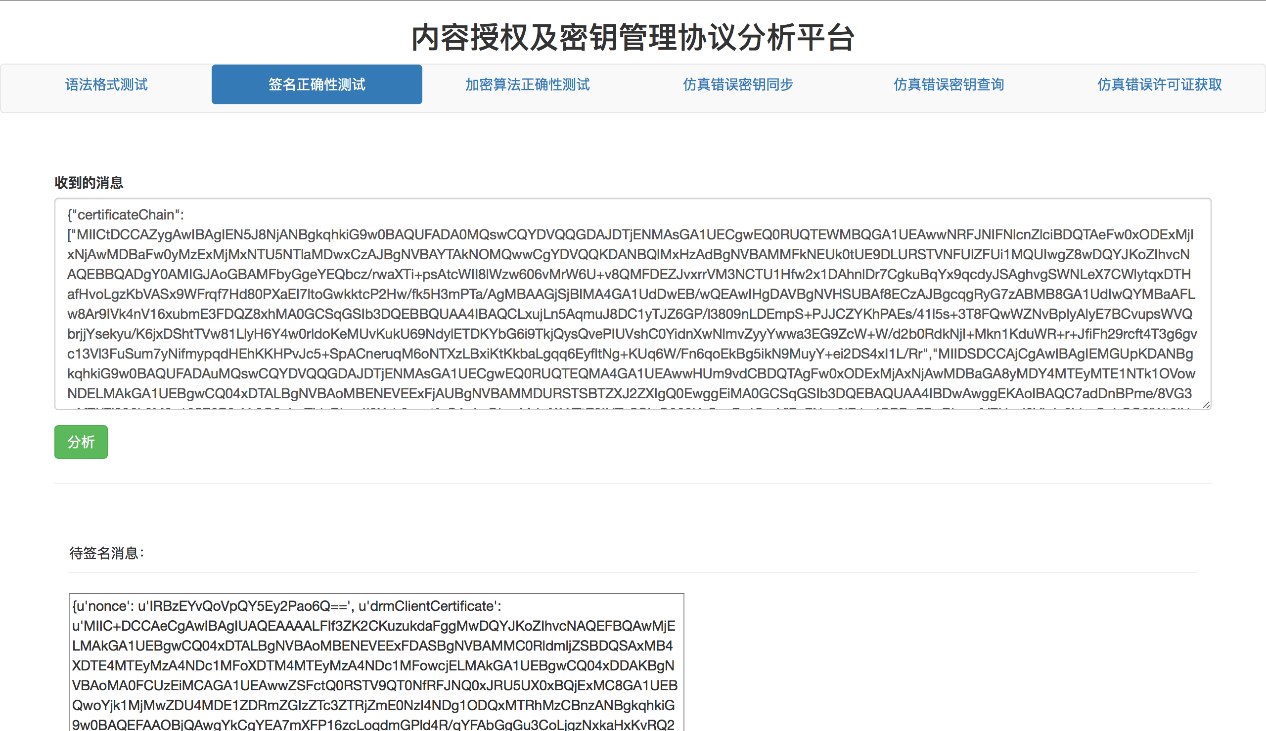
签名正确性分析模块的功能是为许可证获取协议消息、密钥查询消息、密钥同步消息提供签名机制。

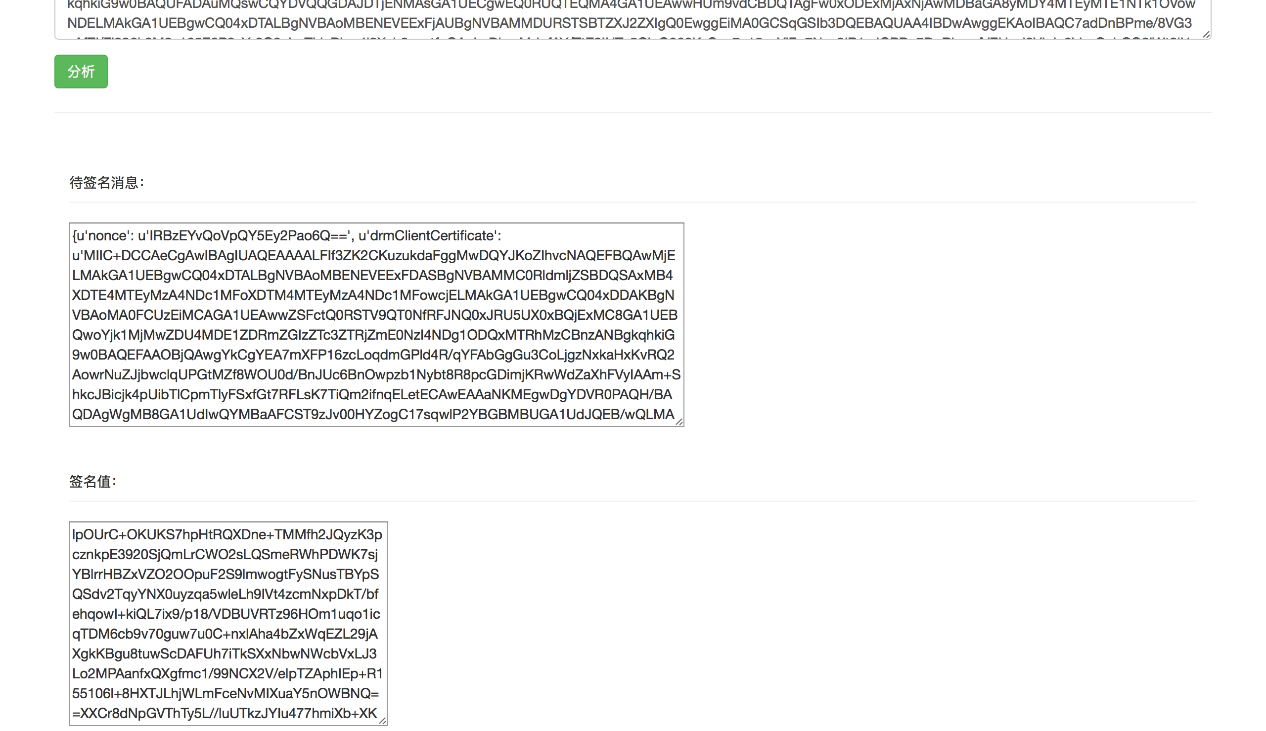
许可证获取协议签名机制：DRM客户端产生签名为空字符串的LicenseRequest JSON String，对该string计算签名，将签名结果填入LicenseRequest JSON String。

DRM服务端产生签名为空字符串的LicenseResponse JSON String，对该string计算签名，将签名结果填入LicenseResponse JSON String。

密钥同步请求中的数字签名使用内容加密方的密钥管理系统的私钥生成。密钥同步数字签名为密钥管理网关使用私钥计算的消息签名。

签名正确性分析部分的界面设计如下：





签名正确性分析界面包括“收到的消息”、“待签名消息”和“签名值”三个文本框，首先将要签名的json文件内容输入“收到的消息”文本框中，点击“分析”按钮，调用后台解析程序，解析出待签名的消息，并且在“签名值”所示的文本框中显示数字签名的内容。