

文件路径加密设计文档

一、设计初衷

避免restapi接口在调用的过程中用到的服务器上的文件存放路径明文传输，暴露服务器文件路径，因此服务器对接口涉及到的服务器存储文件路径的所有参数都采取使用rsa加密算法加密后再进行传输。如下，文件下载接口(/attachment)的file参数加密前和加密后的请求内容对比。加密后文件路径为密文传输到服务器，避免在接口请求过程中暴露真实文件存储路径。**注：仅针对文件路径相关参数的值进行加解密，并非所有参数名和值做加解密**

加密前：<https://192.168.0.100:7443/attachment?file=/opt/data/recorder/files/20241021/1000000000-dd489b50a6144fe19efd850ea7ffed4d-2024-10-21-17-25-51.mp4&token=OWlwYjUyN2QwMzlyNjI4MjM3Yzg2NThlOTdjMzQ5OWNhMDNkZTJkYg==>

加密后：https://192.168.0.100:7443/attachment?file=cLBdRTqpwfM4r7nVKegjUMCGS9hQ.ZZ54ouljhjDE57UzY75p_Pld8Q7pwNlzzYkkK2-SvfT6l2_VYFhfr6k_JNvl4w1ZxUxx7rfPxetXMPXxbLWetMbGy-rBKYHGK6aPkkIKVZAxaBggPT59dkRPMfAQ0qMYRiGEN597rmajut7xldg27nSO84_56ajUTXg8SKO3656jQdlhUOWgU6sB6chLkPaykM_joTrlb6njhf8RxvaehHH_C2_F4hVvfOC2wRcN8OU2c5fMg6UT9Cr6aByvtMBfAZYQOJJ8l6Wt7f9v5EDU1HZEHF4Kxm19xOqgWc4KOVP9nvgh4htch9XJQ==&token=OWlwYjUyN2QwMzlyNjI4MjM3Yzg2NThlOTdjMzQ5OWNhMDNkZTJkYg==

二、启用加密操作方式

在服务器后台管理页面如下图所示可配置是否启用文件路径加密以及加解密使用的公钥和私钥。

注意：1.秘钥仅支持1024/2048位，且私钥格式目前仅支持PKCS1格式

2.如果服务器部署的集群版本则master和media_server需同时开启加密或者同时关闭加密，并且master和media_server要使用同样的公钥和私钥，否则可能出现文件上传下载接口报错。

master后台开启方式：

服务器后台管理系统【集群版】

授权信息: 测试授权, 到期时间: 2079-11-05

平台管理

录制管理

系统管理

安全信息管理

电话网关管理

VoLTE管理

直播管理

授权管理

资源清理

调度管理

集群设置

密码修改

站点管理

信息统计

系统管理 / 集群设置

集群设置 集群地址设置 安全 北向地址设置 平台设置 CPU阈值设置 限流器

安全模式 自定义鉴权 文件路径加密

注释: 上传/下载/录制文件加密

文件路径是否加密 ☒

文件路径加密公钥

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5RJBuFRF73iM3wVMEz/vvCO07EE1hEHmcWHN2EnnPD+zvI9UJV3LOzo4CagdrARMwGC2zI/O+OzNy587F6X7Gc/MaaU76au+KXQowQEfsCwBbTvsPfpLrIlqCC9wEmEhdABd4oJSSd0YVr9iDNoaHC0OpTiKXQH8G02Wz+zR/ZsESPQLB7QJpDTz4Xa+6+571VexUqA1tBNbV0WzYr/gkOaVIN64wAfm02yuJw+aPM4eM3HJ4qO5uq/mi9wXmzMgz3rFN3rwmDJeoZspcEgufdu+WbquR62+htq9Mb3UT1gk5sRZCMSxwoLPKyVehPSVsb455P4H8zIuGT7trhB7wIDAQAB

-----END PUBLIC KEY-----

文件路径加密私钥

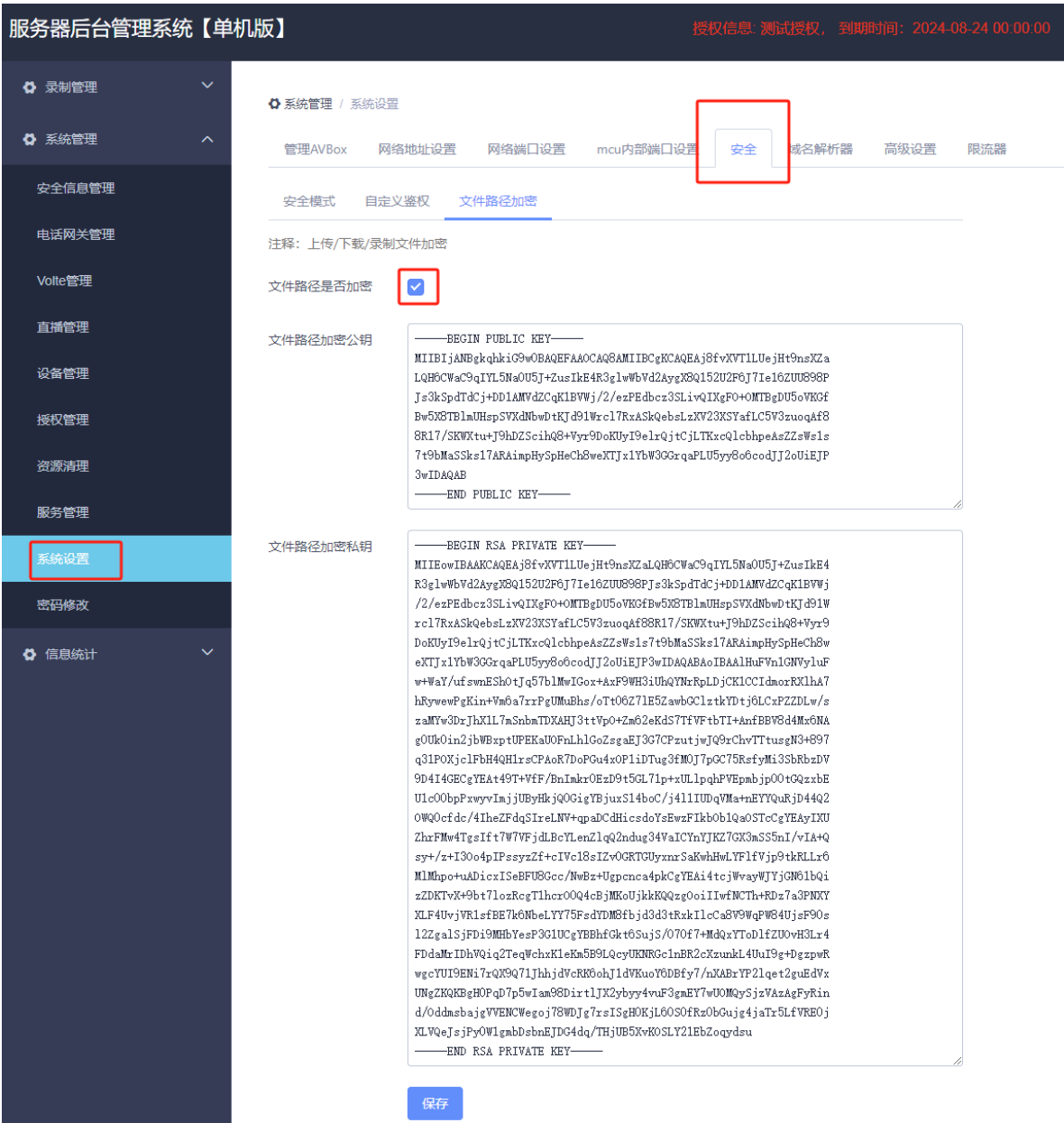
-----BEGIN RSA PRIVATE KEY-----

MIIEPgIBAAKCAQEA5RJBuFRF73iM3wVMEz/vvCO07EE1hEHmcWHN2EnnPD+zvI9UJV3LOzo4CagdrARMwGC2zI/O+OzNy587F6X7Gc/MaaU76au+KXQowQEfsCwBbTvsPfpLrIlqCC9wEmEhdABd4oJSSd0YVr9iDNoaHC0OpTiKXQH8G02Wz+zR/ZsESPQLB7QJpDTz4Xa+6+571VexUqA1tBNbV0WzYr/gkOaVIN64wAfm02yuJw+aPM4eM3HJ4qO5uq/mi9wXmzMgz3rFN3rwmDJeoZspcEgufdu+WbquR62+htq9Mb3UT1gk5sRZCMSxwoLPKyVehPSVsb455P4H8zIuGT7trhB7wIDAQABAOIBAQC9WADgty/ziGaQtdUy/bPwjCIIoMH2p24ujBRU0omDIHiVzLdeB5BETZqiTObvds8Jh92NB5SDEWycKTeLPY1AS/tNMA9ppBJ+zxim9nYswK1GU0fItLKW+YpS29tchKg43z1HLNB0C8HD8y0blrqKkYk33vauIw2o4xLji/bJ5d0eL7N/vKzH5/s01BendOTeqV6ki9ZcezkRln7IxHEZvS3CKJ/bZmvp/zaKJaYx2xGft1bBTR80x0hQFZBABBiiF12fV+JrJO//tYLHdBsf14VZFfs+B9qpkpF3jahhviOD3mtof/Kp4/JfgAejJh4Qq88QPCoppJ08n2RoraIMTJAoGBAPW/KNKVBCrY61B94cdW7EuuTmbDudwERKjTjebMjtdIv3FFIMcDXpqb5UFYyQbSkTF+YmAF6Mzd8mQMwBTE33wdkiCJY8E3De1ofZ8IvF9xVWIFbsDQqwsdXNrbuX0yztvoVPH/Cu14zHCUhTh2QA5gG20WLD8a4EPAG9ZeVy7AoGBAO6g/Gb95XQ0qJLYpcAvhEpVixZEB900kw2IS8TyeTEjz1w3uM8TyXjrui30tq45+emrE27Q4dyKFGJQ2U13tGrh1DEp+B8rmtVMgBmCjm5Nn2Wky9f5hghTPSEsmHAWoenQ+UmXUUVrbbfONxbUmrsQftGsGzRbvBy9JJZDAoGBAO0Jo+ktGwsZ07qtQ8oFGQWetUTuWaHdBBUMKf2LJd5BJFevZBRSLbhsNKIKRjyXjiWUCBXXKmgKOL3hlzAi8d9yUwVRc8Tl3Txms8gKp2ChPexoXP2L2WcUZqt9fvRvaRylaikT5yqKQGVrmDbIo6W7wSMQJ9RfRzqWzT3dafdTaoGBAN6WBbnf/Mb/U3reYQW6jPB1J6xfE4iTdsmd+CeLLUSqB96syQs3NzDFh2KFF32D2rVm7/P1yPCwOFGN8vKHd6cmEryG1kOPtuUzvB5r1FW3Rto4Z4V9SbMki1R7qFqoaWysHsst5Uoyv1k9kvNP6g1kVQxGn7Tej8fWpco818L1AoGBAA0A1GUpraoiORlhRRTyk0byOhdN0yAjMkrRdHT75V7nrE+yNKivHLzdWB04VgEQTVa/ovSevdX5b1WpruwrFQPlm63EEFTu08yNVD3F1kDQkymekIRKYaTpYsf9KJvyWVAq3dgQ3uSFSsjzxp04sCTUj3tXuzzrOPgrJ4RUP8W4

-----END RSA PRIVATE KEY-----

保存

media_server后台开启方式:



三、加解密流程介绍

1.加密算法说明：

对于文件路径加密，服务器采用rsa非对称加密算法，支持秘钥长度为1024位、2048位，私钥格式支持PKCS1。

2.加解密流程说明

- 加密流程：
 - 对原始数据进行rsa加密。
 - 对加密后的数据进行base64编码方便用于restapi接口参数传输

注：考虑到base64后的数据可能会出现"+"、"/"、"="、" "等这些是被URL进行转码的特殊字符，这样就会导致两方面数据不一致,导致前端发送数据请求时,无法跟后台接口正确对接。因此在对加密后的数据base64编码的时候要采用UrIsafe模式（将可能会被url直接转义的符号替换为其他符号，避免被url转义）

- 解密流程：
 - 对base64编码后的数据进行base64解码。

注：base64解码也需要使用UrIsafe模式

2.对原始数据进行rsa解密。

四、涉及sdk接口

文件加解密涉及到以下几个接口和文件路径相关的参数，接口详细参数说明请参考rest api接口文档。

```
/sdkapi/v2/room/get_record // 查询所有录制
/sdkapi/v2/room/get_record_list // 分页查询录制
/sdkapi/v2/room/record/get // 获取录制音频文件
/sdkapi/v2/room/record/get_audio_record// 获取录制音频文件
/sdkapi/v2/room/delete_record // 删除录制
/sdkapi/v2/room/mix_record/stop //停止合屏录制
/sdkapi/v2/room/mix_record/get //获取混屏录制信息及文件路径
/sdkapi/v2/room/desktop_record/get //获取桌面录制信息及文件路径
/sdkapi/v2/web_record/stop //停止网页录制
/sdkapi/v2/web_record/find //获取网页录制信息及文件路径
/uploadfile //文件上传
/attachment //文件下载
```