9 关于 SDK 加密串与用户配置信息安全说明

不推荐将敏感配置加密后写入 SDK

不推荐将 `userid`、`writetoken`、`readtoken`、`secretKey` 加密后随 App 或 SDK 一同分发，也不推荐在客户端解密后再通过 SDK 配置接口传入。

即使客户端保存的是密文，只要密文、解密逻辑或密钥同时存在于 App 中，仍可能被逆向分析获取。因此，客户端加密不能替代服务端密钥管理。

其中，`secretKey` 用于服务端请求签名，必须仅保存在业务服务器的环境变量、配置中心或密钥管理服务中；不得写入 App、SDK 配置、安装包或客户端接口响应。

推荐方案：由业务服务器创建 PlaySafe token

建议由业务服务器完成以下流程：

1. App 向业务服务器提交视频 vid 和必要的身份信息，请求播放授权。
2. 业务服务器校验登录态和观看权限后，使用服务端保存的 `secretKey` 创建 PlaySafe token。
3. 业务服务器将 PlaySafe token 返回 App。
4. App 仅将获得的 token 传给播放器播放加密视频，不保存或使用 `secretKey`、`readtoken`、`writetoken` 等敏感配置。

创建 token 的服务器建议在点播管理后台配置 IP 白名单，仅允许业务服务器的固定出口 IP 调用创建 token 接口。完整流程请参阅 版权保护最佳实践。

已使用 SDK 加密串的应用如何处理

已使用 SDK 加密串或客户端解密方案的应用，建议逐步迁移至服务端创建 PlaySafe token 的方案。迁移期间仍应避免新增或扩散 `secretKey` 等敏感配置到客户端。