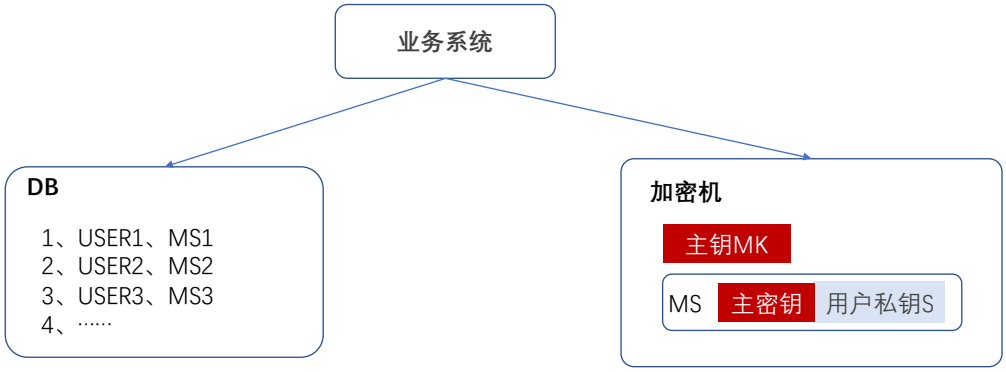
华为项目密钥安全问题解决思路

针对华为安全专家提出的用户私钥运算在明文中出现的问题，我方提出如下解决思路供项目组参考：



需求：服务端签名时，用户私钥明文不在内存中出现，确保安全性。
解决思路：
1、密钥生成：加密机为每个用户生成一个用户私钥S，并使用加密机主密钥Mk加密，形成密文MS。
2、将MS密文存储与数据库中，并对应相应的用户。
3、使用用户私钥运算时（如签名），将MS密文传给加密机，由加密机使用主密钥MK进行内部解密，并完成用户私钥签名运算。

备注：SAFENET 加密机是否支持改该方式需要确认，国内主流加密机普遍支持。