# 国密项目方案决策会会议纪要

|  |  |
| --- | --- |
| **会议时间** | 2018-5-23 9:30--11:00 |
| **会议地点** | 八楼中一会议室 |
| **与会人员** | 夏乔、陆明其、刘青、李学、李永洪、周永华、钟文升、刘三高、刘伟、史磊、郑文豪 |
| **会议主持** | 夏乔 |
| **会议记录** | 冉丽君 |
| **会议主要议题** | 国密场内产品方案讨论会 |

**一、会议议题**

|  |
| --- |
| 1. 国密项目场内产品方案讨论会 |

**二、会议内容**

|  |
| --- |
| **（一）方案介绍**  **要思考这件事给客户带来什么，为客户增强了加密级别，是国家级别的。**  **同时其他外部无法破解。不影响外部、不影响内部升级。**  **李学，将W版与KBSS版加密库进行整合。**   1. **加密随机性的因子，必须要统一。加密加固，时间上的延时需要评估出来。** 2. **接口库，外围是外围DLL，后台**   **后台用的库是包含外围接口，后台用于存储的加解密。外围只有通讯加解密。**  **W版外围调用KDENCODE,后台dll从原来的KDencode换新的dll。**  **U版、KBSS一样，调用通讯加密进来，后台进行通讯解密，存储加密。**  **——确定W版为1个接口库，U版为1个接口库。**  **2.各个产品部门后台调用的接口库文件是否需要统一?**  **答：统一，由一个工程输出的接口库dll或者是.a文件名称一致，并且名称统一为KDSTORAGE.DLL。名称长度需考虑是否有风险。**  **3.各个产品部门后台调用的接口库是否把旧的加解密与国密的加解密函数名分开？**  **答：分开，国密加解密的函数名与原有旧的加解密函数名要分开。——DLL接口方法可以一样，入参默认值送了就是新的，不送就是旧的。**  **4.外围的接口库是否与后台调用接口库统一？**  **答：不需要统一，外围只做dll替换即可文件名不变，但是对应的接口dll要做国密的加密改造。**  **强调：**   1. **对外的，只提供加密函数** 2. **对内的，只提供通讯加解密，存储的加密函数。解密不会对外暴露接口。** 3. **上线要求，外围不需要修改，外围DLL更换后，就是新的加密算法。我们的后台是一起升级吗？**   **账户与各个系统交互，MID等会不会有影响。报盘、银证等相关的都要考虑，升级情况及步骤。自身系统与关联系统的升级顺序。**  **（二）最终结论**   1. 各产品参考W版交易方案，产出各自产品的方案，于两周内完成方案； 2. 各产品柜台客户端增加可查询选择的按钮，增加批量修改功能：能查询哪些客户是老密码，可自主选择迁移，批量修改算法。尽量避免工程操作。 3. 李学需完成各产品DLL加密转换程序，于两周内完成； 4. 各产品后台的dll转为国密算法后都改为统一。 |

会后待办事项：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 待办事项 | 责任人 | 完成时间 |
|  | 收集各产品DLL信息 | 李学、冉丽君 | 2018-4-9 |
|  | 各产品出确定改造方案 | 各产品经理 | 2018-4-18 |
|  | 各产品的白皮书和报价需尽快产出 | 高世博 | 2018-4-13 |
|  |  |  |  |
|  |  |  |  |