# 国密改造项目周例会会议纪要

|  |  |
| --- | --- |
| **会议时间** | 2018-6-4 13:30--15:00 |
| **会议地点** | 八楼中二会议室 |
| **与会人员** | 夏乔、陆明其、李学、王敬普、余跃、谢晓生、麦凤娟、朱文杰、周本高、罗时俊、李永洪、黄磊、郑文豪 |
| **会议主持** | 夏乔 |
| **会议记录** | 冉丽君 |
| **会议主要议题** | 国密改造项目周例会 |

**一、会议议题**

|  |
| --- |
| 1. 总体原则与目标统一 2. 项目待决策问题讨论 3. 后续计划和进度管理 |

**二、会议内容**

|  |
| --- |
| **（一）项目待决策问题讨论**  **1、国密加密库的统一，**   1. **输出密钥没有长度；** 2. **W版nencode level 可以去掉。** 3. **输入都统一成字符型。** 4. **函数返回都是void。** 5. **加密解密重加密是否都需要？** 6. **RC5属于会话，可以放后面改。**   **最终结论：**   1. **U版，加上int P\_inisize，int p\_ioutsize。统一按照U版的出入参。** 2. **函数名修改。加个GM，common encrypt** 3. **有五个函数需要统一：通讯加密、通讯解密、存储加密，以前的存储加密换成现在的国密、对比函数。**   李学研究国际统一标准，出一套参考的标准，大家邮件确认。  **2、旧的加解密的兼容**  国密接口库只包含国密接口，通信加密，通信解密，存储加密，密码类型识别，存储密文转国密，国密密码对比函数。WIN版本因为特殊要求除外。  **（二）其他问题沟通及结论**  **1、封装好的动态库的测试**  动态库需要做白盒测试，测试内容有：稳定性、性能、越界、内存、多线程不要搞乱序等。  ——结论：李学需要写测试用例、测试报告。  **2、李学需要提供开发计划，今日提供。**  **3、函数的应用函数需要有说明文档、加上时序图。李学需要补充。**  4、一柜通的动态库，是否要换掉？  ——需要林毅来定。  5、期权：外围的加密方式，非标准的如何处理？  ——要求客户自己处理。  6、国密通讯解密库，老的密码的兼容，由各产品自己修改？  ——旧密码转换为新密码的转换函数，由李学提供。  7、外围的加密库，什么时候能提供？  ——由李学确定修改计划。  8、外围系统，可能梳理不全。但业务系统必须能保证能兼容旧的模式和新的模式。  9、集成测试，由产品集成部提供集成测试环境。能跑通就可以。  10、明确李学需提供的内容：KDstorage，有5个函数，国密通讯加解密，存储加解密，老的存储密文转新的、类型查询、比对。注意函数是没有明确的导出函数的。 |

会后待办事项：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 待办事项 | 责任人 | 完成时间 |
|  | 由李学提出一套国密标准接口名和出入参供决策 | 李学 | 2018-6-4 |
|  | 李学确定开发计划 | 李学 | 2018-6-4 |