**用户中心安全方案**

1. 全站https

保证数据在网络传输中不会被更改 。

1. 强化ecsc对接口的权限控制，目前只要登录ecsc，就能访问所有接口（包括加载进来的ecmc接口）

即需要前后台的权限校验，目前只有前台有权限校验。

1. 涉及用户金额的业务，金额不以前台传入为准。根据前台传入的计算因子，在后台重新算过。
2. 消息队列改用专业消息队列工具，需要带消息确认机制，不用redis。
3. 业务数据安全，定时全量备份mysql，redis。
4. 与外部系统交互，要验证对方身份（特别是支付结果回调通知）
5. 涉及金额变动的业务，做好业务失败的处理，以便重新执行。
6. 分布式锁，解决金额变动的数据正确性。
7. 对余额表的操作：update table set 余额=余额+变化量
8. 涉及金额变动业务，记录好日志，备查。
9. 各服务停机机制。
10. MQ消费者使用规则：
    1. 基本原则：取消息🡪做业务🡪发确认消息
    2. 异常处理：
       1. 因为生产者事务没提交导致消费者取不到数据的，消费者等待，比如100次循环，每次等待50毫秒，再取不到的，记录日志，发确认消息。
       2. 处理过程出现异常的，记录日志，发确认消息。