**摘要:** 【问题】 在企业信息化推进的过程中，需要建设许多的信息系统，这些系统能够实现高效率、低成本的运行，为企业提升竞争力。但在设计和实现这些信息系统时，除了针对具体业务需求进行详细的分析，保证满足具体的业务需求之外，还要加强信息系统安全方面的考虑。因为如果一个系统的安全措施没有做好，那么系统功能越强大，系统出安全事故时的危害与损失也就越大。 请围绕“信息系统的安全性与保密性”论题，依次从以下三个方面进行论述： 1.概要叙述你参与分析设计的信息系统及你所担任的主要工作。 2.深入讨论作者参与建设的信息系统中，面临的安全及保密性问题，以及解决该问题采用的技术方案。 3.经过系统运行实践，客观的评价你的技术方案，并指出不足，以及解决方案。 【摘要】 2018年3月，本人所在的公司承接了一套代付系统的建设。该项目主要业务是接收各个上游服务的代付请求，通过某个第三方代付通道进行实际出款。本人在该项目中担任了架构师的职位，负责该系统的架构设计。本文以该项目为例，主要论述了信息系统的安全性和保密性设计。在交互报文设计方面，为了防止报文信息泄露、篡改和抵赖问题，我们采用了数字信封的策略；在数据库存储方面，为了防止数据信息泄露以及篡改，采用敏感信息加密保存、记录摘要字段的策略；在登录认证方面，为了增加安全强度，我们采用了用户密码、图形验证码、手机验证码、Ukey四项策略来实现登录认证。通过以上技术方案的实现，系统的安全性和保密性达到了很好的效果，最终项目顺利上线，稳定运行。

2018年3月，本人所在的公司承接了一套代付系统的建设。该系统的核心业务点是将接收到的代付请求，审核通过后，通过第三方代付通道将钱实际发出去。该系统分为四大子系统：前置服务，用于接收上游系统发送过来的代付请求报文，验证通过后记录入库；代付通道服务，该服务内对接了多个第三方代付通道，风控清算等一系列部门审核通过后，该服务将钱实际代付出去；路由服务，该服务是根据不同的代付业务场景，以及每个代付通道的实际资金情况等，选择把每个代付流水分配到哪个第三方代付通道进行出款；管理平台服务，该服务的内容比较多，包括代付流水的查看、代付流水的审核、证书管理、第三方通道信息管理、报表服务等。因为该系统中存在着大量的敏感信息，比如银行卡号、银行卡户名、身份证号、手机号等，所以该项目的安全等级必须设计为最高等级。本人在该项目中担任系统架构师一职，负责该项目的架构设计工作。  
代付系统中，因为业务的敏感性，涉及到很多的敏感信息，比如说银行卡号、户名、身份证号、手机号等，这些敏感信息都需要在网络中进行传输，也会在数据库里进行保存，因此数据的安全性和保密性问题面临着巨大的挑战，网络传输的过程中有可能被非法采集，数据库被拖库的情况下也会导致信息泄露；业务场景是把钱真实的代付出去，涉及到上游系统或者机构的抵赖问题，每一笔交易报文都要让对方无法抵赖；接口报文在传输过程中绝对不能被篡改，否则实际出款数据就完全错了；报文接口也要考虑到重放攻击的可能，报文重放，签名也挡不住，会导致重复处理代付的问题；业务系统在处理的过程中，也存在着泄露信息的风险，比如说日志系统，如果说日志文件中记录了敏感信息的明文，就有可能存在日志文件被窃取导致信息泄露；管理平台服务的操作都是很敏感的，所以管理平台的登录认证功能也必须做到最高安全等级，一旦登录入口被攻破，后果难以想象。  
以上列出了部分系统中涉及到的安全性和保密性问题，针对这些问题，我们采用了对称和非对称算法的加解密、计算信息摘要、报文签名策略、日志脱敏打印、物理设备Ukey、防止重放攻击、https协议等一系列安全防控策略。下文着重讨论接口报文层面、数据库存储层面、登录认证层面所面临的问题以及我们采用的解决方案。  
一、接口报文层面  
代付项目中的报文，含有大量的敏感信息，包括银行卡号、户名、身份证号、手机号等，这些都是一级敏感数据，绝对不能在报文传输过程中被非法收集到。在实际业务场景方面，一笔报文请求的到来，意味着要把真金白银给发放出去，所以对上游系统的身份验证也必须做到最高的安全等级控制，防止对方抵赖不认可。针对以上问题我们决定采用数字信封技术进行解决。报文加密方面，因报文的数据量比较大，采用对称算法进行加密，每笔请求随机生成一个对称算法的秘钥加密报文，该对称秘钥采用对端的公钥进行加密传输，做到一笔一个随机加密秘钥，提高加密安全性。身份验证方面，将报文明文进行摘要签名，签名结果随报文一起上送，用于身份验证，签名串在数据库中也会进行存储，防止对方抵赖。加密和签名解决了，还有一个很重要的重放攻击需要防御，我们在报文内部加了唯一流水号以及时间戳信息，流水号必须全局唯一，在数据库层面做了唯一索引控制，业务系统上判断如果时间戳和当前时间相差超过30秒直接作为失败处理。  
二、数据库存储层面  
代付项目中的数据，都是极为敏感的，数据库中绝对不能明文存储，防止数据库被拖库后信息泄露，针对这一场景，我们决定对每个敏感字段进行加密存储。前置服务在收到代付请求后，把敏感字段信息加密后存储，后续的各个业务服务，都是只能使用密文来进行业务中转处理。加密防止信息泄露解决了，但是数据库还有一个大问题需要解决，防止数据篡改，如果说数据记录里的卡号、姓名、金额等信息被篡改，那这笔钱代付就完全错了，这个影响是不可接受的。针对这一问题，我们把每条数据记录额外计算一个摘要信息字段进行存储，数据在入库前，把关键性字段（卡号、姓名、金额等）拼接起来，再使用一个系统内部自定义的秘钥串作为盐，然后计算一个摘要结果一起入库保存，后续任何业务场景中读取出数据记录后，第一步就是重新计算摘要信息，如果发现和数据库里记录的不一致，拒绝处理。  
三、登录认证层面  
代付系统的管理平台服务，可以进行流水的查看、导出、秘钥证书管理等，都是极为敏感重要的操作，稍有不慎，后果就会很严重，因此该平台的首要入口登录认证就要严格控制。首先是用户名、登录密码、图形验证码基本三要素进行判断；其次是手机验证码控制，每次管理员登录时，系统都会发送手机验证码到管理员信息表里预设的手机号上，该手机号验证码验证通过才可以，防止管理员密码丢失导致他人恶意登录；再一层次是每个管理员都分配了一个单独的物理Ukey，该Ukey里保存着一个单独的私钥数据，管理员每次登陆的时候，系统都会调用Ukey生成一个签名数据送到服务端，服务端使用该管理员的公钥进行签名验证，该ukey为一个物理硬件，除非丢失，否则不可能被窃取，如果认为丢失了，可以在平台商直接禁用掉该管理员即可。通过手机号验证码和Ukey的引用，登录认证模块的安全性可以达到最高的层次。此处我们也加了防止重放攻击的措施，防止报文被截取到直接重放。  
该项目历时13个月，于2019年4月上线，一直持续稳定运行，未出现过安全事故，也未曾反应泄露过数据。前置服务接收代付请求模块中，后续经历了好多次的攻击，都是签名验证失败给挡掉了，目前未碰到重放攻击的，后续即使遭遇到重放攻击，系统也可以识别出进行防御。前置接口的攻击，虽然被签名验证给过滤了，但是大量的签名验证请求，严重消耗CPU资源，针对这一情况，我们在前置服务里加入了IP白名单的限制，如果是非IP白名单的报文请求，系统直接拒绝处理。关于证书的管理，考虑到相关人员定期有离职的情况，为了防止证书泄露，系统中使用到的证书和秘钥，我们都要求定期进行更换，虽然麻烦，但是必须做到安全第一。安全和性能一直就是对冲的属性，需要去平衡，但是针对该系统而言，安全必须做到最高，性能我们可以适当放弃，项目后期压力测试时，性能不是很满意，后续商讨决定，安全等级不能降，通过集群部署的方式来增加系统性能。  
系统安全是一个永久的话题，我们对系统的完善改进也是一个持续的过程，后续我们还会继续观察改善系统安全性方面的问题以及不足，使整个代付系统更加的安全可靠。