|  |
| --- |
| **Ipay支付系统安全交易的设计和实现** |
|  |
|  |
| 团队：popcorn |
|  |
| **梁建均** |
| **2011/9/1** |
|  |

# 摘要和引言

## 摘要

安全问题是电子商务的重要部分，一个良好的安全交易方案保证电子交易的高效和安全。当前，主流的相关安全技术有SET和SSL两种。其中SSl协议实现较为简单，但是存在一定安全隐患；而SET协议安全度高，但是实现起来比较昂贵。不管使用哪种技术，都应该参考系统的具体实际情况，定制适合系统的安全方案。Ipay支付系统参考这两个协议，考虑实际情况（如技术难度，开发时间，硬件性能），设计和实现一个安全的交易方案。

## 引言

Ipay支付系统安全交易的设计涉及到密码散列算法，数据加密算法和非对称加密算法等技术，参考SET和SSL协议，调用java类库自带的部分安全类库来实现安全支付。支付过程中除了保证支付过程的安全加密，还要避免用户粗心失误导致的安全漏洞，同时要兼顾网络环境和算法的效率。

# 网上支付安全性的要求

* 有效性。预防和控制计算机软硬件及网络的错误，以保证贸易数据在确定的

时刻、确定的地点是有效的。

* 机密性。防止非法的信息存取和信息在传输过程中被非法盗窃。
* 数据的完整性。预防对信息的随意生成、修改和删除，同时要防止数据传送

过程中信息的丢失和重复并保证信息传送次序的统一。

* 可靠，不可抵赖性。在无纸化的电子商务方式下，通过手写签名和印章进行

贸易双方的鉴别已是不可能的。因此，要在交易信息的传输过程中为参与交易的个人、

企业或国家提供可靠的标识。

* 审查能力。根据机密性和完整性的要求，应对数据审查的结果进行记录。

# 安全措施

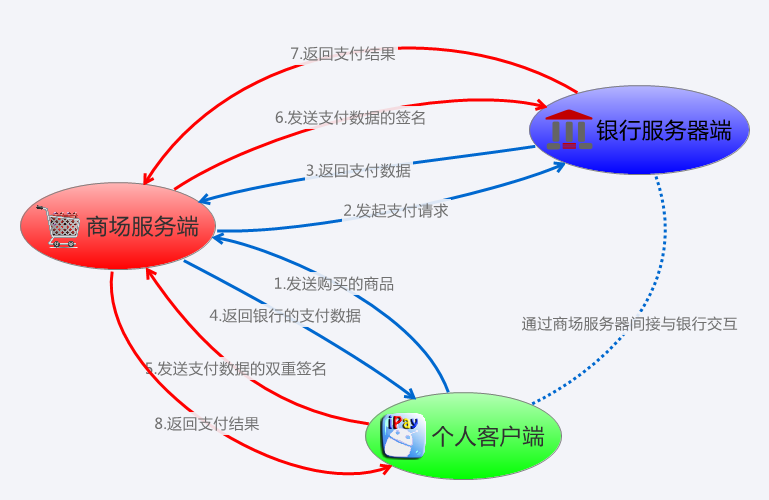
电子商务中一般采取以下的安全措施：

* 数据加密。保证数据的安全。
* 认证。为了确定发送者的身份。
* 交易放抵赖。发方不能否认曾向收方发过信息，收方不能在收到信息后否认

已经收到信息。

* 授权。决定用户是否有权执行某一项特殊的操作。

# ipay支付流程设计



* 注册阶段

个人客户端和商场服务端都需要经过注册阶段，此阶段将获取相关信息，保存起来。

（1）个人客户端在注册时需要获取银行的公钥（公开）以及经过支付密码加密的银行卡的私钥（保密）

（2）商场注册时需要获取加密的银行卡的私钥，并且重新加密，保存到商场服务器端。银行数据库要存有所有的银行卡（包括个人和商场）的公钥和使用支付密码加密的私钥

* 支付阶段

支付过程中使用https加密连接：

1. 个人客户端把需要购买的订单（orders）发送到商场服务器。商场计算需要支付的费用。
2. 商场把商场信用卡和需要支付的费用通过银行公钥加密以及对这些信息进行签名发送给银行（RSAencrypt(market cardnum+amount)+RSAsign(market cardnum +amount)），银行验证并且生成支付浩（tranid）。
3. 银行用商场的公钥加密支付号和要支付的费用，返回给商场，同时返回这些数据的签名（RSAencrypt(tranId+amount)+RSAsign(tranId+amount)），商场验证信息并且使用使用查看这些信息。
4. 商场把银行的支付请求返回给客户端（RSAencrypt(tranId+amount)+ RSAsign(tranId +amount)），客户端查看并验证这些信息，然后等待用户输入支付密码，解密私钥，并用私钥对这些信息进行签名，确认支付。
5. 个人客户端对支付数据进行双重签名，（RSAencrypt(OI)+RSAencrypt(PI)+ RSAsign(OI)+RSAsign(PI)+RSAsign(OIMD+PIMD)），发送给商场。商场验证里面的OI信息。
6. 商场把客户端的支付数据继续发送给银行，让银行处理，银行验证签名和数据，然后把修改保存到数据库。
7. 银行返回支付结果，以及对结果的签名，（RSAencrypt(result)+RSAencrypt(result)+ RSAsign(result），商场根据支付成功与否保存购买记录。
8. 商场把支付结果返回给客户端，客户端根据支付结果显示提示信息给用户。

# ipay支付流程实现

其具体实现的代码请参考源代码。其中加密用到的工具已经在:

项目IpayMarketServer的com.ipay.server.security类库中

项目IpayBankServer的com.ipay.server.security类库中

项目IpayClient的com.ipay.security中

# 其他影响因素

* 由于网络的不稳定，应该考虑支付过程中出现网中断的处理，除了提高硬件环境外（如增强wifi热点的负载能力），还应该增加对数据的完整性验证和支付中断的撤销操作等
* 客户端为用户提供自动登录和帐号密码保存服务时要意识到客户端存在的诸多不安全因素，如客户端中毒，非法程序窃取数据，被人恶意盗窃手机等问题。所以应该增加更多的提醒，及时通知用户潜在的不安全因素
* 为保障整个系统的稳定，可以尝试增加更多安全手段，例如支付时要使用短信发送临时的支付密码，三次输错密码就冻结帐号。

# 参考文献

1. 郭中华，徐飞 基于SSL协议的SET协议模拟实现
2. 吴波 易协议的网上支付系统的设计和实现
3. 黄元飞 信息安全与加密解密核心技术.

【4】 梁栋 Java加密与解密的艺术