# 密码学原理与实践
# （32实践部分）

# 1、目的

- 熟悉软件开发过程
- 撰写完整的设计文档
- 网络编程，网站开发
- 应用密码学知识理论完成认证、加密
- 最终提升软件开发能力

# 2、任务

① 简单的网上交易系统、虚拟支付系统和认证服务系统的设计及代码实现；
② 网上交易、虚拟支付、认证服务安全协议设计；
③ 用户身份认证模块设计及代码实现；
④ 数据加密模块设计与代码实现；

# 3、课程实践过程及评分

① 成绩，平时表现10分+软件60分+报告30分

② 第1次课，分组，每组3人，每人完成一个模块，最后三部分要协作展示；

③ 完成需求分析、概要设计（第2次上课时，每组做一个ppt，分为三部分，三人一起上来讲解你们的方案，讲清楚三人如何接口，协调工作）；

④ 40学时，每人独立开发软件，每组协商接口，三人联动演示（软件60分：完整性10分，安全部分30分，美观10分，合作10分）；

⑤ 提交完整的开发电子文档（30分）（需求分析，概要设计，详细设计，测试报告）

- ✓ 完整性20分，排版10分

# 成绩分布

| 平时成绩（10） | 软件成绩 | | | | | | 系统文档（30） |
|---|---|---|---|---|---|---|---|
| | 传输安全（10） | 存储安全（10） | 身份认证（10） | 美观（10） | 合作（10） | 完整性（10） | |
| 平时测验及回答问题。 | 解决端到端的传输加密问题；方案合理，实现了相关代码，测试通过 | 解决数据存储的加密问题；方案合理，实现了相关代码，测试通过 | 解决系统的用户身份认证问题；方案合理，实现了相关代码，测试通过 | 软件界面美观，有较好的易用性，操作流畅。 | 组内三人，软件能够协作运行，实现安全电子商务 | 系统具备常见的主要功能，能够较好地实现预定功能。 | 文档包含概要设计、详细设计、代码实现说明，测试；结构合理，图表清晰，语言通顺 |

注：实验成绩为百分制，实验成绩计入课程总成绩的 40%。

# 4、环境

- 题目
  ① 虚拟支付系统（网上银行）
  ② 基于互联网的电子商务平台
  ③ 认证服务系统
- B/S结构，C/S结构，包括两部分：服务器和客户端，且不在一台机器上
- 客户端平台windows （B/S），android（C/S），
- 开发语言java、php、c＋＋，等语言等，
- 客户端界面，浏览器、图形化客户端、手机，基于微信亦可。

# 5、基本的开发文档

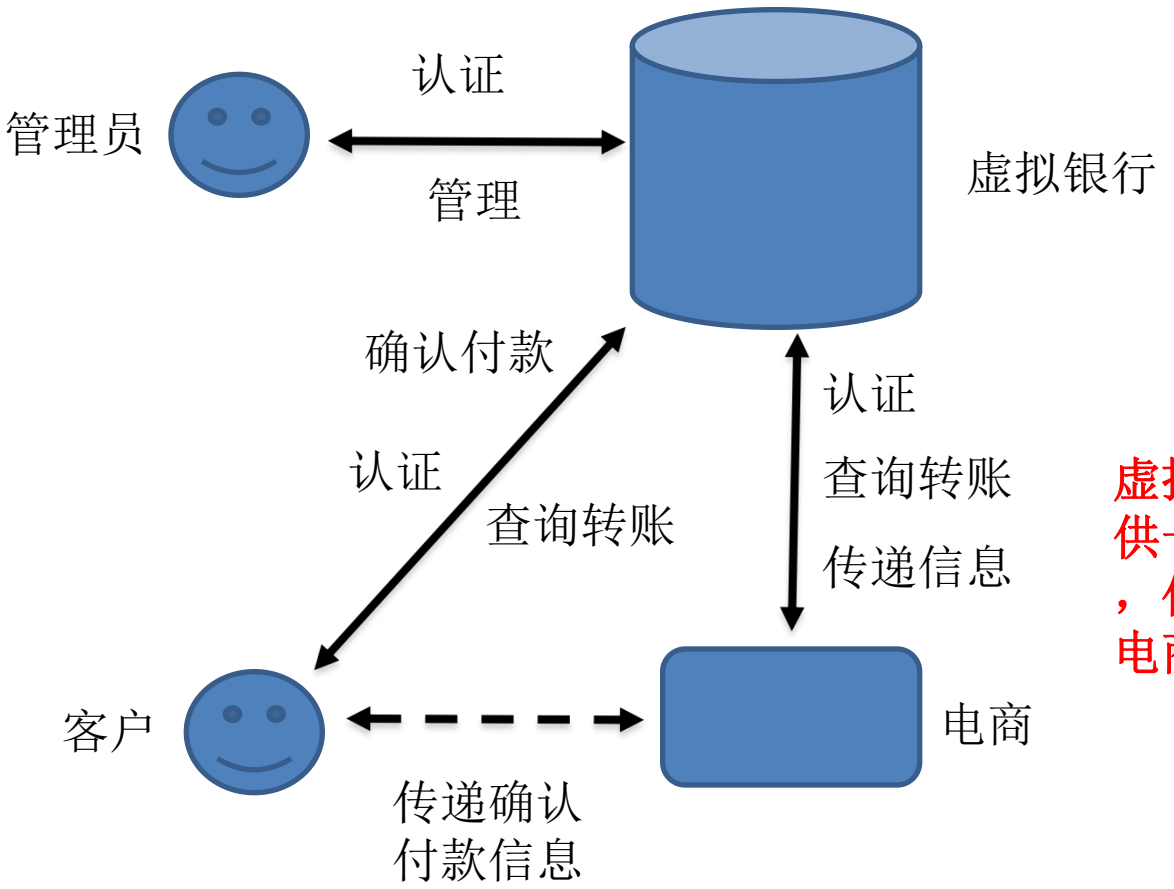
- 需求分析：软件要做什么，具有什么功能
- 概要设计：依据需求分析，设计如何实现这些功能，功能模块化分。
- 详细设计：展开概要设计，详细描述每个功能模块的具体实现。
- 测试报告：详细测试每个功能、每项性能。

总的来说，以上就是软件设计的各个阶段主线。

# 6、虚拟网络银行的基本功能

❶ 建立帐户，帐户之间可以转帐；（全部加密）
❷ 身份认证，较强的安全性；
❸ 用户接口，用户可以查看用户状态，进行存取业务；
❹ 交易接口，顾客点击“付款确认”，交易平台调用此接口（给出个链接），并提供付款额度、顾客信息（银行名）和双签名信息（仲裁凭证）给银行，进入银行网站，顾客输入帐号和认证凭证，银行审批交易，然后转帐，／＊此步需要传输安全，及隐私保护。
❺ 通知交易平台，付款完成。

# 软件架构

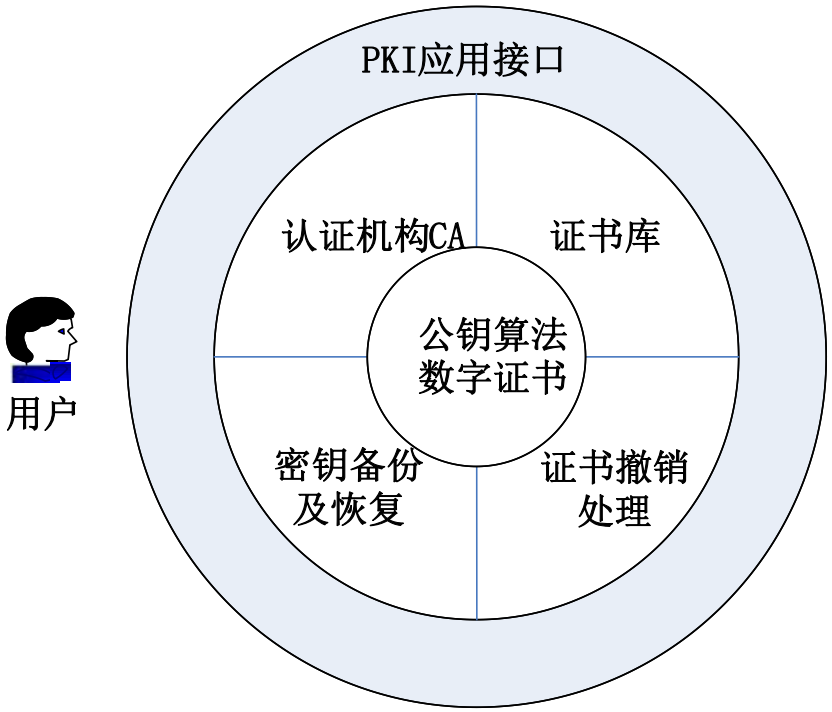


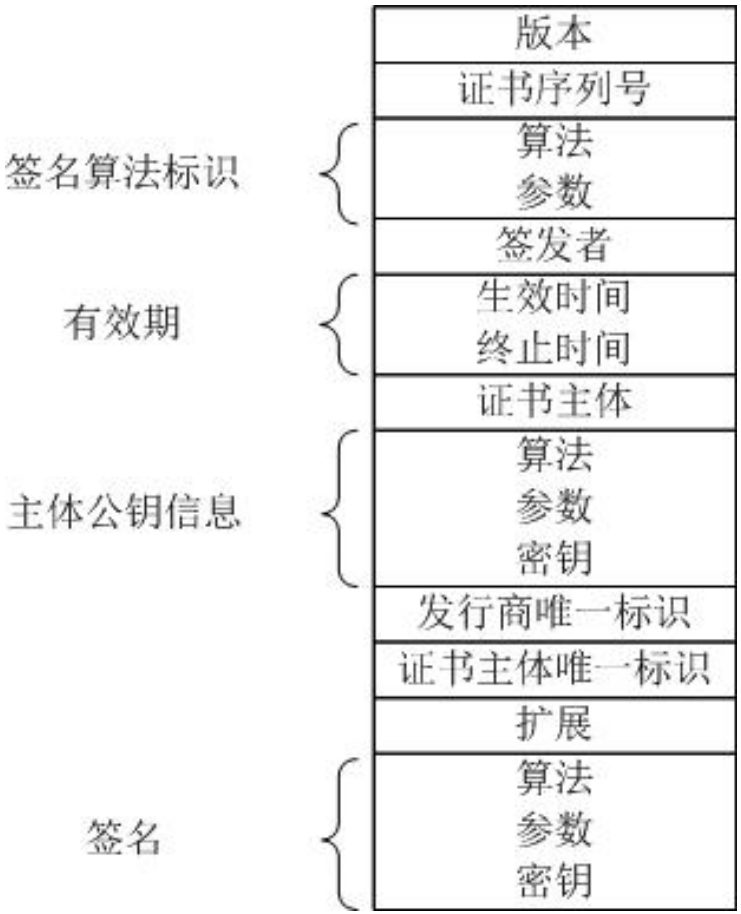

虚拟银行提供一个借口，付款，供电商使用

# 7、认证服务系统的基本功能

- 接收验证用户数字证书的申请；
- 生成证书
- 存储证书
- 向申请者颁发（或拒绝颁发）数字证书；
- 接收用户数字证书的查询、撤销；
- 产生和发布证书的有效期；
- 数字证书的归档；
- 密钥归档；

# 软件架构

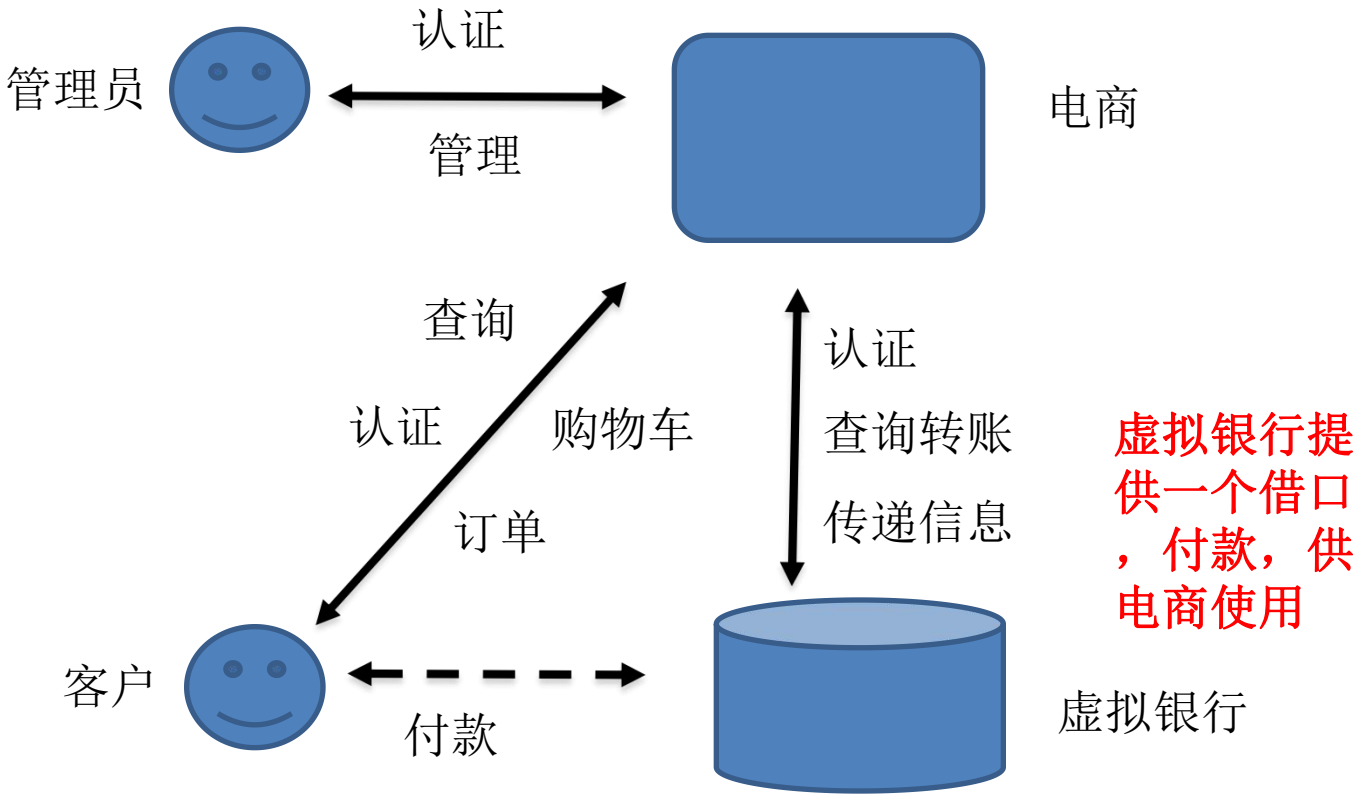

PKI应用接口
认证机构CA
证书库
公钥算法
数字证书
密钥备份
及恢复
证书撤销
处理
用户
管理员


版本
证书序列号
签名算法标识
算法
参数
签发者
有效期
生效时间
终止时间
证书主体
主体公钥信息
算法
参数
密钥
发行商唯一标识
证书主体唯一标识
扩展
签名
算法
参数
密钥

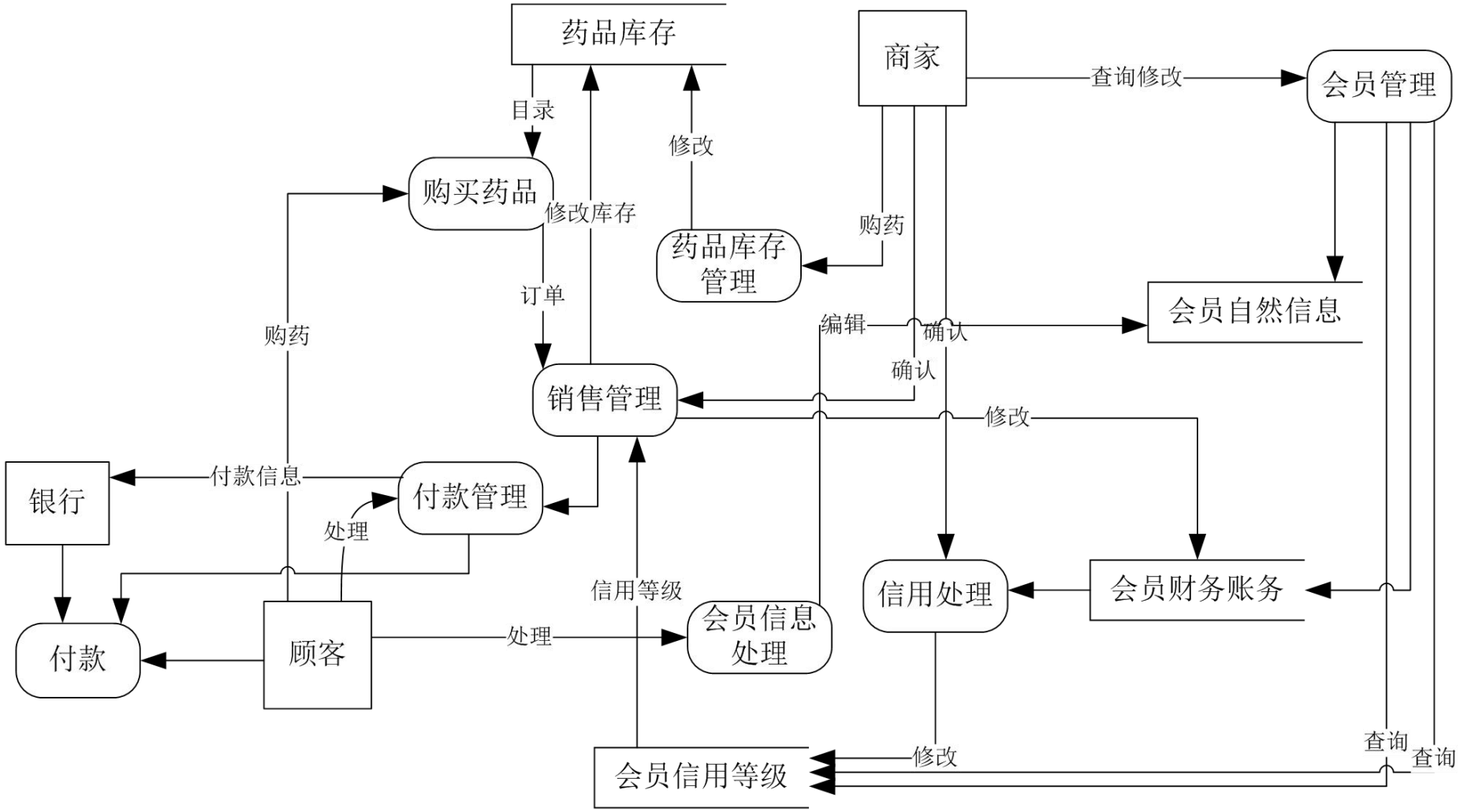
# 8、基于互联网的电子商务平台

❶ 商品信息列表
❷ 购物车
❸ 买家身份认证（加密）
❹ 买家帐户注册及维护（加密）
❺ 订单确认（加密）。
❻ 付款确认（加密），连接调用虚拟支付系统的接口。
❼ 完成交易，接收支付系统发来的付款完成信息后，交易成功，确认发货，并通知买家；长时间未收到的付款完成信息，取消订单，并通知买家。

# 功能逻辑架构


管理员
认证
管理
电商
查询
认证
购物车
订单
认证
查询转账
传递信息
虚拟银行提供一个借口，付款，供电商使用
客户
付款
虚拟银行

# 9、例子


药品库存
商家
查询修改
会员管理
目录
修改
购买药品
修改库存
购药
药品库存管理
订单
会员自然信息
购药
编辑
确认
确认
销售管理
修改
银行
付款信息
付款管理
处理
信用处理
会员财务账务
信用等级
付款
顾客
处理
会员信息处理
修改
查询
查询
会员信用等级

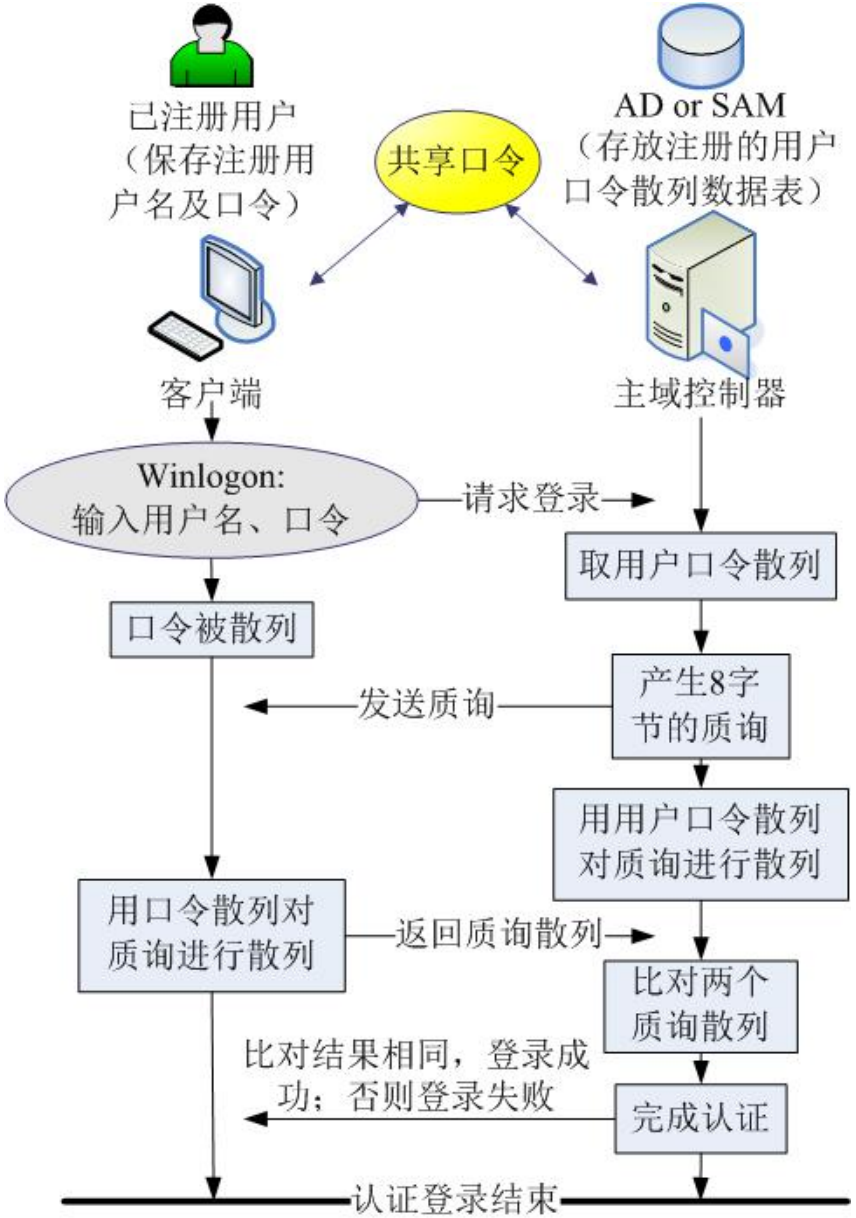
# 10、关键技术

- 认证
  - 认证方式：普通密码、校验码、手机、图形、短信、软键盘等
  - 认证安全协议
- 传输
  - 哪些数据传输时需要保密，如何保密
- 注册
  - 远程注册是如何实现隐私数据安全
- 数据库安全
  - 保证数据库重要数据安全，如密码、分片等。

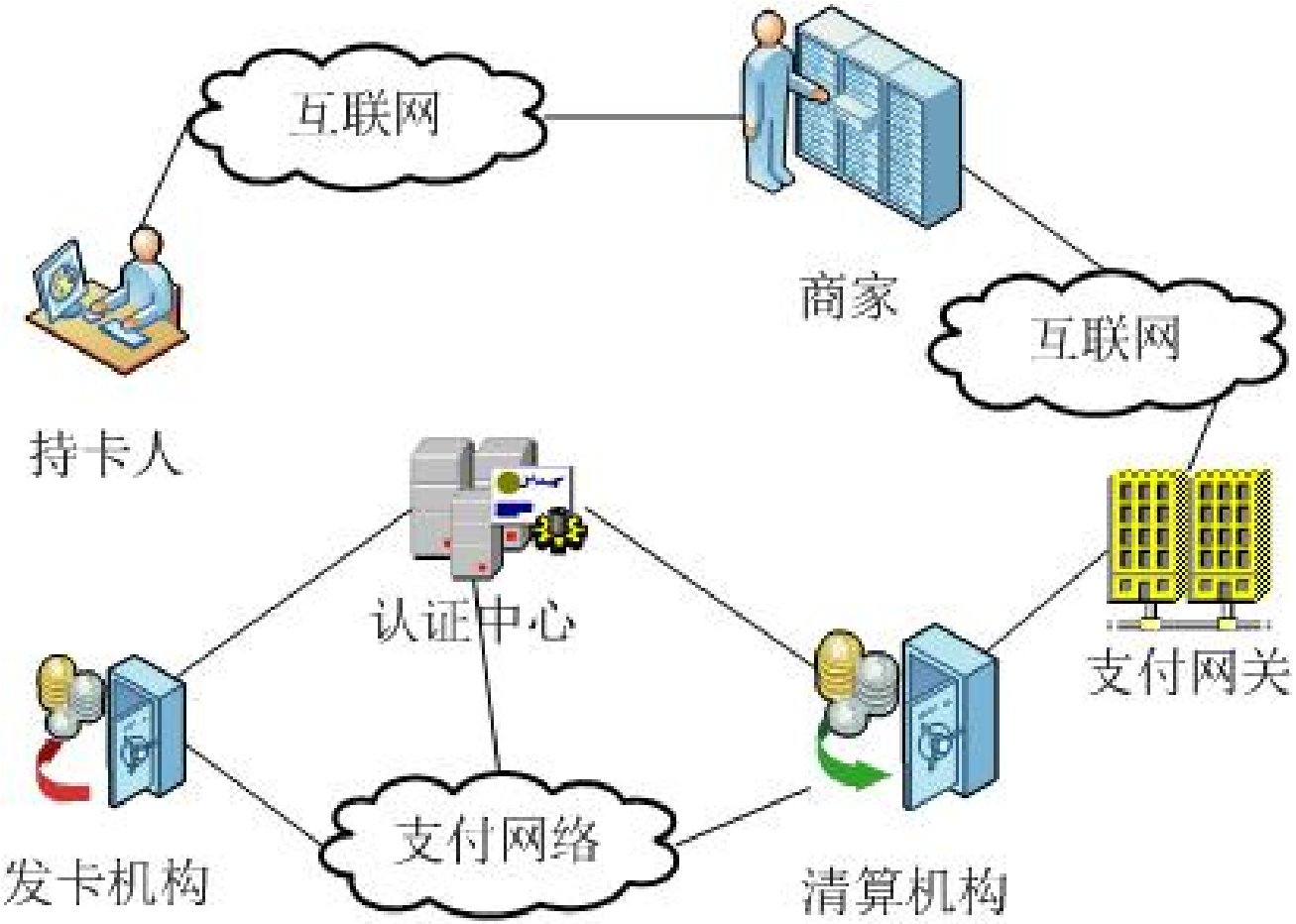
# 10、关键技术

- 隐私信息保护
  - 隐私信息：属性信息、状态信息、行为信息等
  - 隐私外延：私人、小群体、大群体、
  - 信息隔离：例如：银行与商家，信息传递
- 支付接口设计
  - 参数传递：链接加参数，其他如信息串推送。

# 11 windows登陆认证



# 12、安全电子交易协议SET



# 安全问题及安全技术

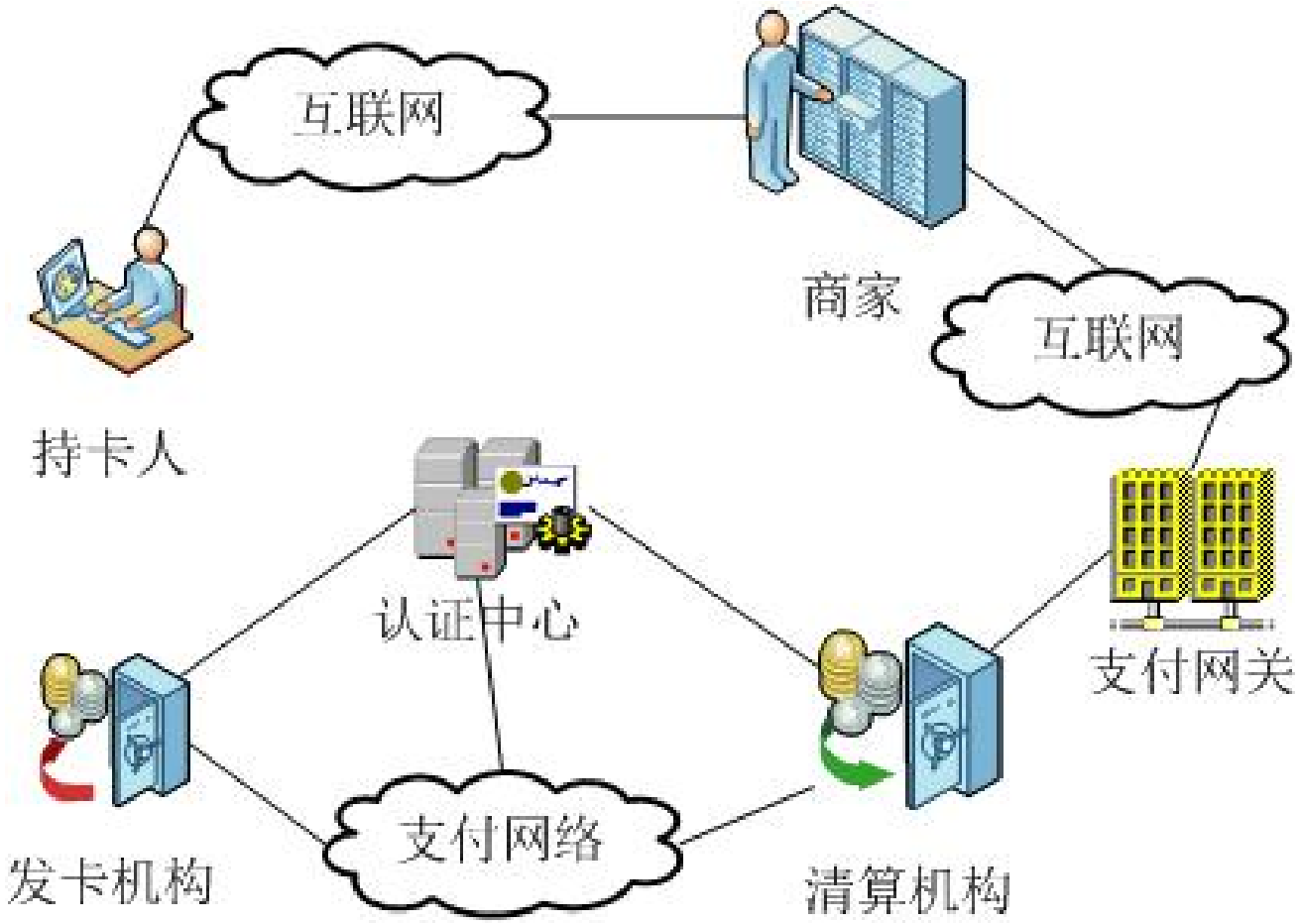
- 面临的安全问题
  - 用户注册，身份认证，认证，信息交互，交易
    - 有效性
    - 真实性
    - 机密性
    - 不可否认性
    - 完整性
- 安全技术
  - 加密技术
  - 认证技术
  - 完整性
  - 安全协议
  - CA认证

# SET协议概述

- SET（Secure Electronic Transcation）
  - Visa和MasterCard发起，联合IBM、Microsoft、Netscope、GTE等公司
- SET安全协议的目标：
  - 保证交易信息在互联网上安全传输，防止数据被黑客或被内部人员窃取。
  - 保证电子商务参与者信息的相互隔离。客户的资料加密或打包后通过商家到达银行，但是商家不能看到客户的账户和密码信息。
  - 持卡人和商家相互认证，以确定通信双方的身份，由第三方机构负责为在线通信双方提供信用担保。
  - 保证网上交易的实时性，使支付过程都是在线的。
  - 要求软件遵循相同协议和报文格式，使不同厂家开发的软件具有兼容性和互操作功能。

# SET的组件结构

- SET的六组件
  - CardHolder、Merchant、Issuer、Acquirer、Payment Gateway、Certificate Authority



# SET的安全机制

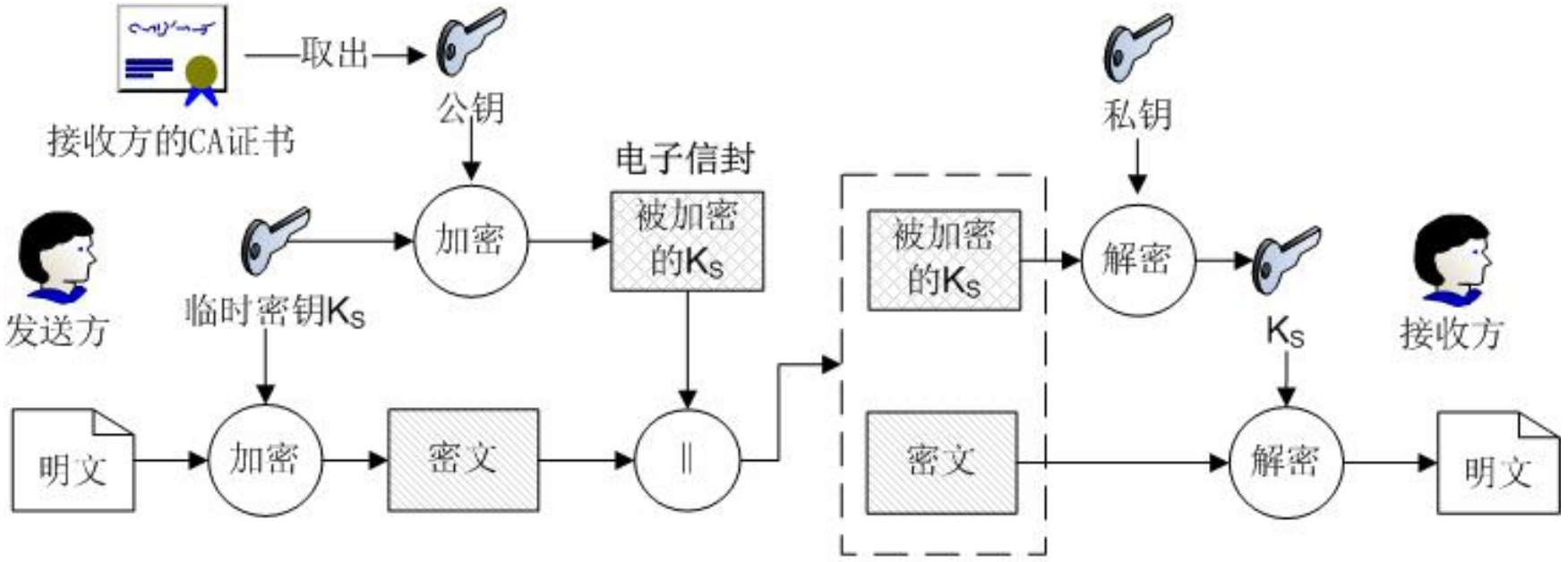
- SET协议安全性主要依靠其采用的多种安全机制，
  - 对称密钥密码
  - 公开密钥密码
  - 数字签名
  - 消息摘要
  - 电子信封
  - 数字证书
  - 双重签名
- 安全机制解决了包括机密性、完整性、身份认证和不可否认性等问题，提供了更高的信任度和可靠性。

# CA证书

- CA证书就是一份文档，它记录了用户的公开密钥和其他身份信息。
- 最重要的证书是持卡人证书和商家证书。
- 还包括支付网关证书、清算机构（银行）证书、发卡机构（银行）证书。
- 这些证书均由一个权威的CA签发，如某金融机构的认证中心。

# 电子信封

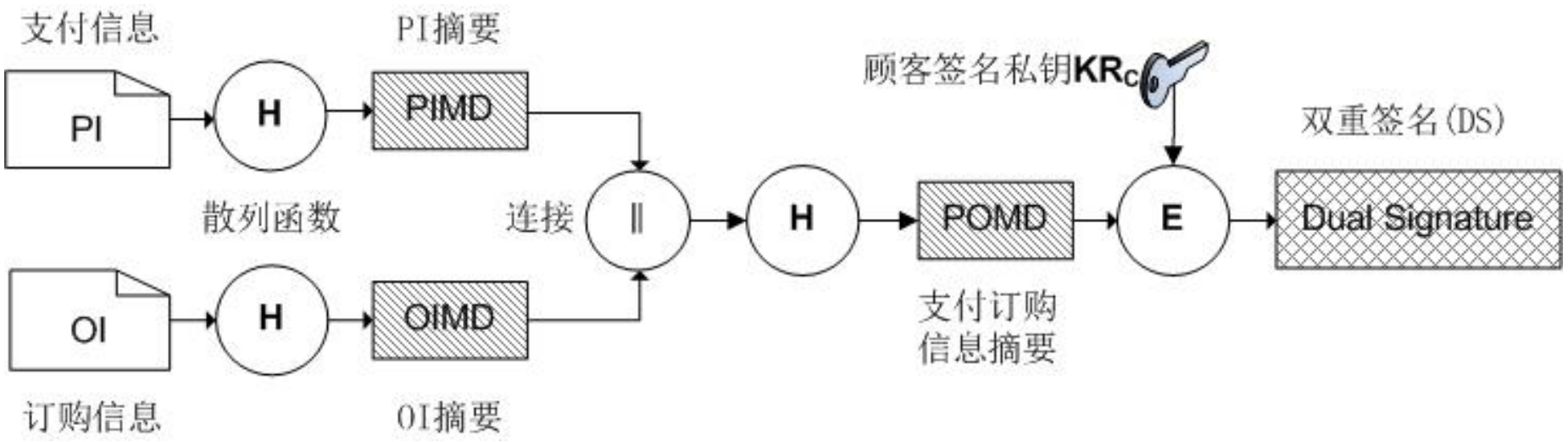
- SET协议使用电子信封来传递更新的密钥
- 电子信封涉及到两个密钥
  - 一个是接收方的公开密钥
  - 另一个是发送方生成临时密钥（对称密钥）




电子信封的使用过程

# 双重签名

- SET协议核心内容是订购信息OI和支付信息PI
- DS（Dual Signature）技术将OI和PI这两部分的摘要信息绑定，确保电子交易的有效性和公正性
- 分离PI与OI，确保商家不知道顾客的支付卡信息，银行不知道顾客的订购细节。
- $DS = E_{KRc}[\,H(H(PI)\ \ H(OI))\,]$



# 双重签名的使用过程

- 顾客针对PI和OI生成DS，将DS、OI和PIMD发送给商家，
- 商家计算得到POMD=H（PIMD　H（OI））， 然后计算POMD’=$D_{KUc}$ [ DS ]，其中KUc为顾客的公开密钥。如果POMD= POMD’,则商家可以认为该DS正确，批准实施进一步交易
- 顾客需要生成一个对称密钥$K_S$，使用银行的公钥加密$K_S$，并使用$K_S$加密DS、PI和OIMD，通过商家将$E_{KUb}$ [$K_S$]　$E_{Ks}$[ DS　PI　OIMD ]转发给银行
  - 其中KUb为银行的公开密钥
- 银行计算POMD=H（H（PI）　OIMD）和POMD’=$D_{KUc}$ [ DS ]，如果POMD= POMD’,则银行可以认为该DS正确，批准实施交易。

# Any Question?