## 数据库表的设计

### 软件信息表

软件信息表software主要用于保存与软件相关的信息，softwareName指的是实际软件的名称（包含后缀名），实际软件被保存在工程的softwares目录中。softwareType指的是软件系列名称，每个系列有多个权限等级，价格的单位是元。

表4.9 软件信息表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 字段名 | 字段说明 | 类型 | 长度 | 允许空值 | 备注 |
| softwareId | 软件Id | int | 10 | 否 | 主键 |
| softwareName | 软件名称 | varchar | 200 | 是 |  |
| softwareDescripe | 软件描述 | text |  | 是 |  |
| price | 软件价格 | int | 11 | 是 |  |
| permissionLevel | 权限等级 | int | 11 | 是 |  |
| softwareType | 软件类型 | varchar | 200 | 是 |  |

### 软件订单表

软件订单表orders包含着用户购买软件时的全部信息，订单号对应提交的订单，订单号不允许重复，主要有submit\wait\finished三种交易状态。同时还在表中设有软件Id、用户Id作为外键，用于对软件信息表、用户信息表进行关联。

表4.10 软件订单表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 字段名 | 字段说明 | 类型 | 长度 | 允许空值 | 备注 |
| orderId | 订单Id | int | 11 | 否 | 主键 |
| softwareId | 软件Id | int | 11 | 是 | 外键 |
| usersId | 用户Id | int | 11 | 是 | 外键 |
| tradeNo | 订单号 | varchar | 64 | 是 |  |
| serialNo | 流水号 | varchar | 64 | 是 |  |
| tradeState | 交易状态 | varchar | 20 | 是 |  |

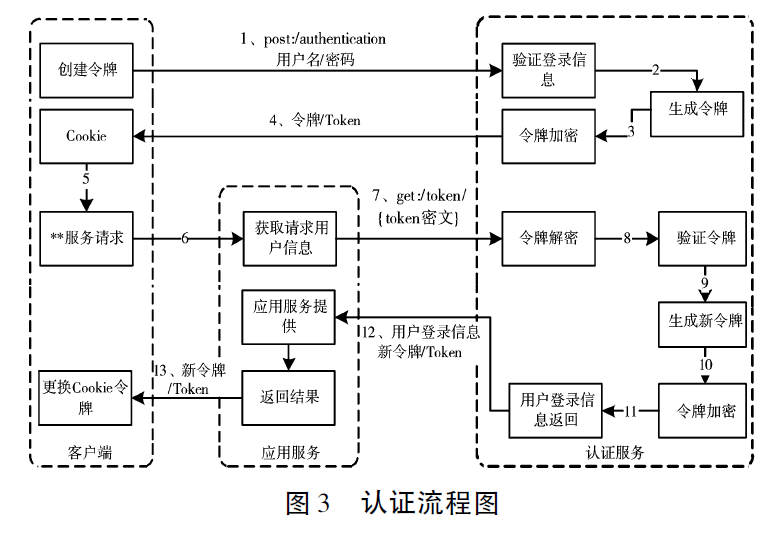
### 交易日志表

交易日志表pay\_log在每次用户提交、修改或者完成订单的时候，插入一条记录，做为交易日志，以备日后审计查阅。

表4.11 交易日志表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 字段名 | 字段说明 | 类型 | 长度 | 允许空值 | 备注 |
| id | 日志Id | int | 11 | 否 | 主键 |
| userName | 用户名 | varchar | 20 | 是 |  |
| outTradeNo | 订单号 | varchar | 64 | 是 |  |
| subject | 订单名称 | varchar | 64 | 是 |  |
| price | 价格 | int | 11 | 是 |  |
| tradeNo | 流水号 | varchar | 64 | 是 |  |
| tradeStatus | 交易状态 | varchar | 20 | 是 |  |
| response | 返回信息 | varchar | 30 | 是 |  |
| time | 修改时间 | timestamp | 14 | 是 |  |

## 认证过程



(1) 新用户通过客户端向认证服务器端发出创建令牌资源的请求( POST: /authentication) ，请求的表单中内容包含用户名和密码等认证信息;

(2) 服务器端对用户信息进行认证，通过认证后，将登录用户信息作为令牌一部分，生成用户Token，同时在数据库users中保存tokenID;

(3) 对令牌进行加密，形成加密后的密文令牌;

(4) 将加过密的令牌返回给客户端;

(5) 当客户端向其它应用服务提出任何服务请求时，都需将Cookie 中的令牌一起提交给应用服务器;

(6) 应用服务收到令牌后，向认证服务请求令牌解析服务( GET: /token /{ token 密文} ) ，将加密后密文作为令牌资源的ID 提交给认证服务;

(7) 认证服务根据密钥将密文解密，成功解密认为Token 是合法的，否则认为Token 非法;

(8) 认证服务根据令牌里的tokenID与数据库中的tokenID相比较，相同是合法的，否则认为非法;

( 9) 认证服务根据新的请求时间重新制作新Token;

(10) 将新Token 经过同样加密，变为密文;

(11) 如果认证通过，则将令牌中的登录用户信息返回，同时将新生成的令牌返回应用服务;

(12) 应用服务获取登录用户信息，完成后续请求的应答;

(13) 应用服务将认证服务返回的新令牌通过Cookie 设置方式替换客户端的旧令牌，应用服务器端也不保存用户的登录信息。这样客户端在下次向应用服务发出请求就使用新的令牌，重复(5) 到(13) 步骤.

## 支付流程

