金融终端权限系统设计报告

摘　要

本文阐述整个金融终端系统的权限控制，涉及到客户端权限控制，服务端权限控制，版本权限控制。

关键词： 功能 ；菜单；资源； 命令；限定；角色；掩码

目　录

1 引言

1.1 设计背景

基于对不同用户,不同产品的功能权限需求以及按产品和组合功能模块的销售模式及服务的安全考虑，需要引入授权中心来满足细粒度的权限控制需求。

1.2 设计意义

通过引入权限控制系统，既能做到客户端的用户权限控制，又能做到不同系统间调用的权限控制以及数据内容的权限控制。

1.3 设计方法

从数据，接口，API 的权限基本单元出发进行抽象，将所有需要控制的单元统称为“资源”，对资源进行各种操作(增加，删除，修改，查询)的控制，通过对各种操作进行有条件的控制(操作限定)。

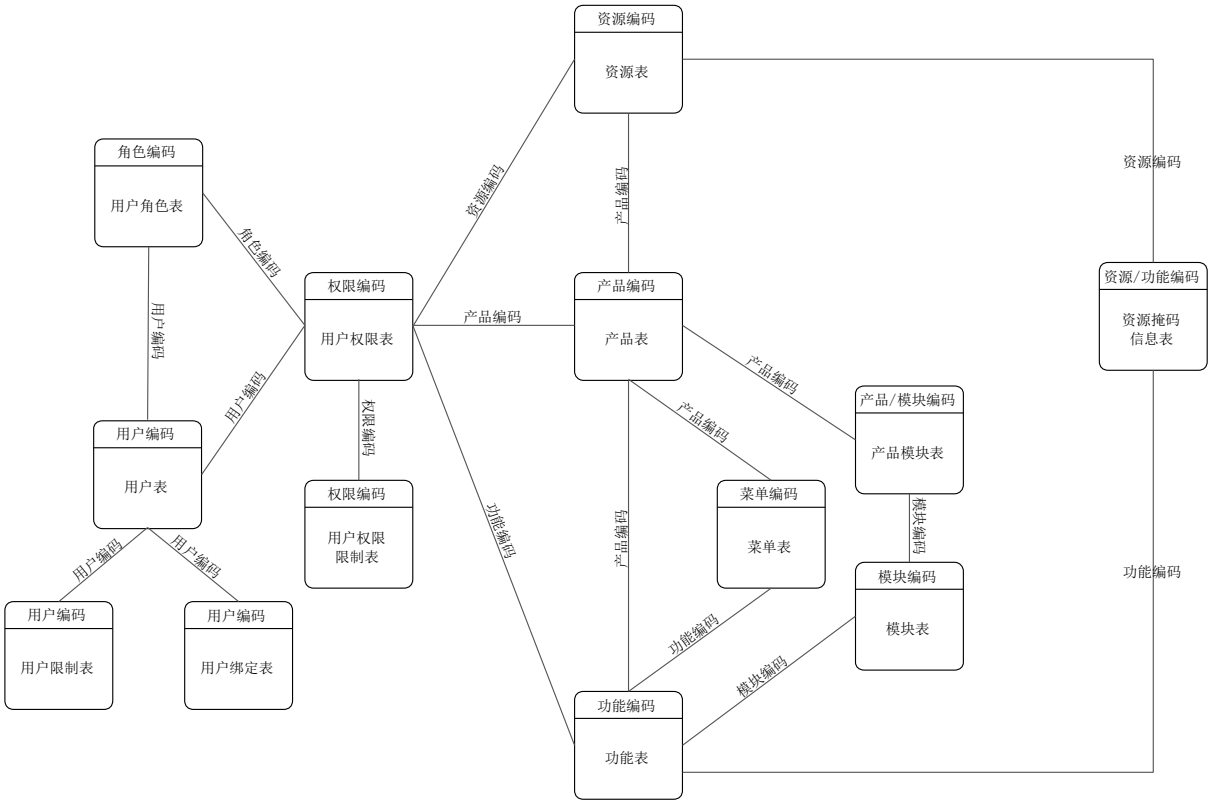
1.4 目的及内容

本报告主要阐述权限系统中的涉及的表结构以及表之间的关系以及如何通过权限控制系统进行服务接口和客户端功能权限控制的逻辑。

2 系统设计

2.1 表设计

系统非关键表(登陆日志表，行为操作表)不在表设计中描述。



2.1.1 产品表

系统需要支持多产品的权限控制，对每个产品均有具体的定义。

产品表 (AC_ ProductInfo)			
字段	类型	名称	备注
ProductCode	Varchar(38)	产品编号	唯一标识，用来区分产品
ProductName	Varchar(100)	产品名称	
ProductShortName	Varchar(50)	产品简称	
ProductDesc	Varchar(200)	产品介绍	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.2 类库表

类库表记录了各个类库的信息，有利于多产品的模块组装和打包。

模块表 (AC_ LibraryInfo)			
字段	类型	名称	备注
LibraryCode	Int	类库编码	唯一标识，用来区分类库
LibraryName	Varchar(100)	类库名称	
LibraryDesc	Varchar(200)	类库描述	
DevAuthor	Varchar(100)	类库开发者	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.3 模块表

系统支持各种终端的权限控制(PC,Web,APP)，需要对客户端的模块进行划分，如专题模块，数据浏览器模块，宏观模块，深度资料模块。即使一个 Library 对应多个模块，也需要对模块进行定义，如果一个模块需要多个 Library 的，可以定义为基础模块(系统核心支撑)。

模块表 (AC_ ModuleInfo)			
字段	类型	名称	备注
ModuleCode	Int	模块编码	唯一标识，用来区分模块
ModuleName	Varchar(100)	模块名称	
ModuleDesc	Varchar(200)	模块描述	
LibraryCode	Varchar(100)	类库编码集合	支持多个 Library
ModuleCmd	Varchar(50)	模块命令	
ModuleParam	Varchar(50)	模块参数	模块参数
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.4 产品模块表

不同的产品有不同的模块，每个模块都是基于一个或多个统一的 Libraray 完成，所以可以将不同的模块组装成不同的产品。

模块表 (AC_ ProductModuleInfo)

字段	类型	名称	备注
ProductCode	Varchar(38)	产品编码	
ModuleCode	Int	模块编码	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.5 功能表

系统中每个功能都会找到一个模块对应，每个模块存在对应多个功能，如 Web 模块，可以支撑 新闻功能，研报功能，公告功能，行情模块，对应了 60，F5，F3，F1 等功能。

功能表 (AC_ ModuleFunctionInfo)			
字段	类型	名称	备注
FunctionCode	Int	功能编码	唯一标识，用来区分功能
FunctionName	Varchar(50)	功能名称	
FunctionCmd	Int	功能命令	
FunctionParam	Varchar(100)	功能参数	用来关联类库
ModuleCode	Int	模块编码	用来关联模块
ResourceCode	Varchar(200)	资源编码	允许 NULL，关联资源编码，用来进一步控制控能对资源的访问
FucntionDesc	Varchar(200)	功能说明	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.6 资源分类表

任何一个权限单元都被抽象成资源，不同类别的权限单元被划分到不同的资源分类中，如：前端功能，后端接口，数据。

资源分类(AC_ ResourceCategory)			
字段	类型	名称	备注
CategoryCode	Int	分类编码	唯一标识，用于关联
CategoryName	char(50)	分类名称	
PCategoryCode	Int	父分类代码	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.7 资源表

权限控制的最小单元就是资源，任何一个需要权限控制的都可以称之为资源，大到产品，小到接口中数据

资源(AC_ ResourceInfo)			
字段	类型	名称	备注
ResourceCode	Int	资源编码	唯一标识，用于关联
CategoryCode	Int	分类分类编码	关联资源分类表

ResourceName	Varchar(30)	资源名称	
ResourceDesc	Varchar(50)	资源描述	
ResourceParam	Varchar(100)	资源配置	用于资源的统一控制
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.8 菜单表

菜单本身并不是权限控制的单元，但菜单是权限控制的一种表现形式，菜单是功能的一种入口方式。

菜单(AC_ MenuInfo)			
字段	类型	名称	备注
MenuCode	Int	菜单编码	菜单的唯一标识
PMenuCode	Int	上级菜单编码	用来建立菜单树
MenuCnCaption	Varchar(50)	菜单名称	
MenuEnCaption	Varchar(50)	菜单英文名称	用于语言切换
MenuImage	Varchar(50)	菜单图标名称	用户更换图标
FunctionCode	Int	关联的功能	菜单一定关联功能，但功能不一定关联菜单，菜单只是功能入口的一种方式
HotKey	Varchar(50)	菜单的快捷键	
MenuType	Int	菜单类型	如横向，竖向，分组等，预留根据实际需求配置
HintInfo	Varchar(100)	菜单的提示信息	
Favorite	Varchar(50)	菜单收藏名称	
OrderNum	Int	菜单顺序	
IsDisplay	Bool	是否显示	
DisplayStyle	Int	显示样式	根据实际需求定义其中菜单的样式
ProductCode	Int	关联产品编码	
ProductVersion	Int	关联的产品版本	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.9 资源掩码信息表

通过掩码对每个需要权限控制的资源进行更细分的控制，如对一个资源的四项操作（增，删，改，查）。

掩码信息(AC_ ResourceMaskInfo)			
字段	类型	名称	备注
ID	Int	标志性 ID	唯一标识，自增
CategoryCode	Int	资源分类	区分哪种类型的掩码，如：前端的功能，后端的资源都具有掩码的权限控制。

ResourceCode	Int	资源编码/功能编码	
Mask	Int	掩码定义	值为2^n,n[1..31],值 1 为功能的默认掩码
Desc	Varchar(50)	掩码描述	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.10 用户权限表

此表是用户权限控制的核心表，也是权限查询的入口点，通过此表将用户与产品，资源，功能产生联系。

用户权限(AC_UserRightInfo)			
字段	类型	名称	备注
ID	Int	权限 ID	唯一标识，自增
UserCode	Int	用户编码/角色编码	
ProductCode	Varchar(50)	产品编码	
Mask	Int	权限掩码	
CategoryCode	Int	资源分类编码	
ResourceCode	Int	资源编码	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.11 用户权限限制表

虽然通过了资源的掩码对资源进行了更细粒度的划分，但是仍然不能进行数据的细粒度划分，如对某个资源的查询权限进行数据的权限控制—某个用户能查询 A 条件的股票，某个用户能查询 B 条件的股票，此时 A 条件和 B 条件是不能通过掩码进行控制的，掩码仅支持 31 位，意味着有 31 种权限控制。

用户权限限制(AC_UserRightRestrictInfo)			
字段	类型	名称	备注
RightID	Int	权限 ID	关联用户权限
MaskBit	Int	权限掩码位	
Restrict	Varchar(200)	限制条件	根据某个资源自身定义
Info	Varchar(200)	描述	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.12 角色表

系统管理中需要支持角色的权限控制。

角色(AC_RoleInfo)			
字段	类型	名称	备注

RoleCode	Int	角色编码	
RoleDesc	Varchar(50)	角色说明	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.13 用户角色表

系统管理中需要支持角色的权限控制。

用户角色(AC_UserRoleInfo)			
字段	类型	名称	备注
ID	Int	ID	唯一标识
RoleCode	Int	角色编码	
UserCode	Int	用户编码	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.14 用户表

系统管理中需要支持角色的权限控制。

用户表(AC_UserInfo)			
字段	类型	名称	备注
UserCode	Int	用户编码	
UserName	Varchar(50)	用户姓名	
LoginName	Varchar(20)	登陆名	全部以 G 开头
LoginPassword	Varchar(50)	登陆密码	SHA1 加密
Mobile	Varchar(11)	手机号	可作为登陆名
Email	Varchar(30)	邮件	可作为登陆名
IsActivate	Bool	是否激活	
UserType	Int	用户类型	0：外部用户，1：内部用户
ValidStartDate	DateTime	用户有效日期	
ValidEndDate	DateTime	用户结束日期	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.15 用户限制表

系统管理中需要支持角色的权限控制。

用户表(AC_UserRestrictInfo)			
字段	类型	名称	备注
UserCode	Int	用户编码	
RestrictType	Int	限制类型	0:限制数量，1:限制 IP 点，2:限制 IP 段
RestrictNum	Int	限制数量	
RestrictIp	Varchar(50)	限制 IP	

EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.1.16 用户绑定表

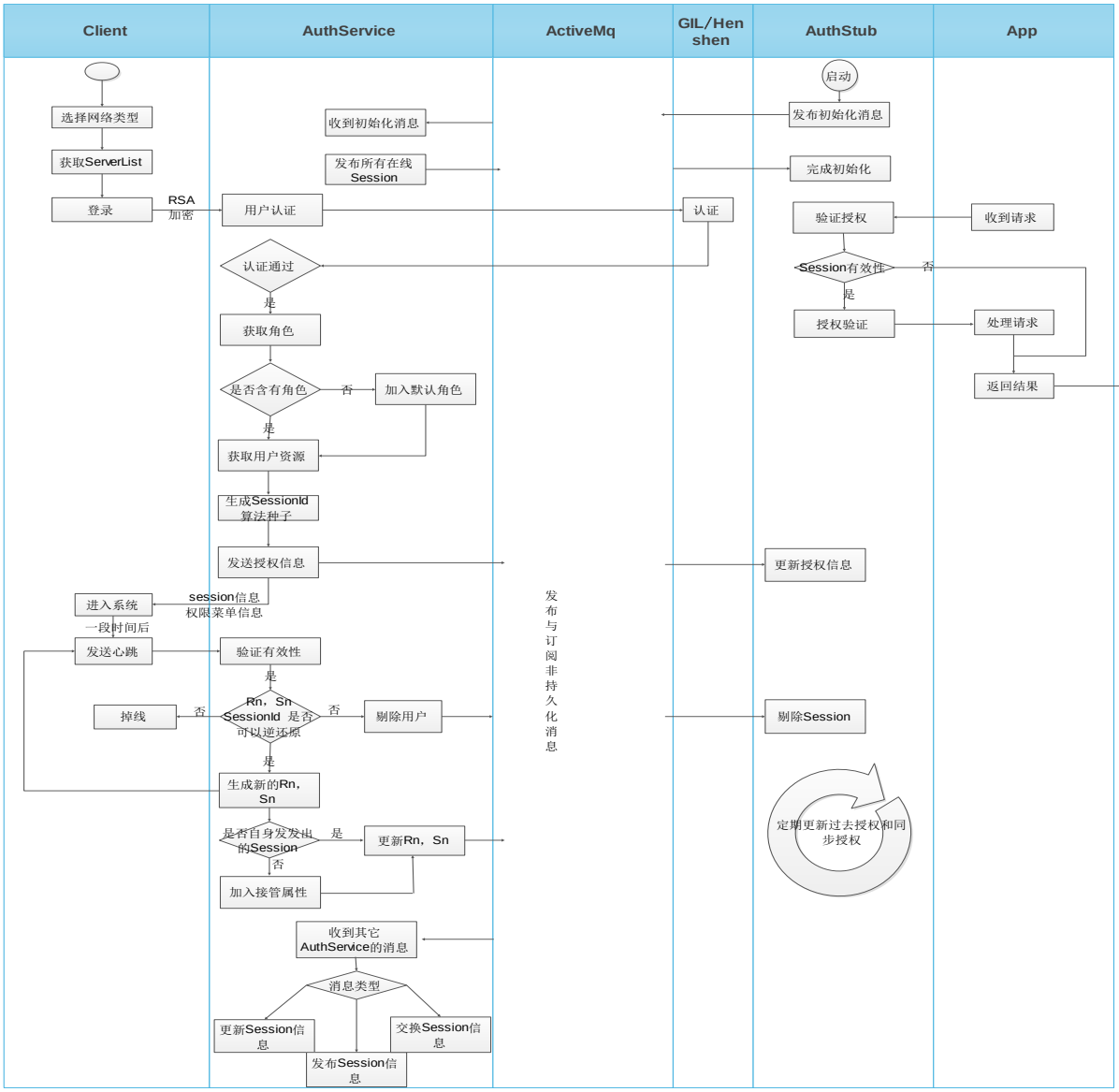
用户绑定表主要用来绑定用户机器。

用户表(AC_UserBindInfo)			
字段	类型	名称	备注
UserCode	Int	用户编码	
ProductCode	Int	产品编码	
CpuID	Varchar(30)	CPUID	
HardiskID	Varchar(50)	硬盘 ID	
MacID	Varchar(30)	MacID	
ComputerName	Varchar(30)	计算机名	
LoginName	Varchar(30)	登陆名	
EntryTime	TimeStamp	进表时间	
SyncState	Int	同步状态	用户测试到生产上数据同步

2.2 登陆设计

系统采用单次登陆，Session 验权的模式进行，其中认证又可以交给其他系统进行认证。

2.2.1 授权流程



2.2.2 状态码定义

返回码	作用
101	已经接收客户端的请求，但客户端的版本已经不再维护范围内，需要客户端做更新操作后再进行登录
200	完成客户端的验证请求。
201	用户完成验证请求，客户端完成初始化后弹出一个消息框。
400	请求的参数中缺少必要的参数，服务器无法理解请求结构。
401	用户不存在，客户端提示申请注册试用账户。
402	密码错误，客户端提示找回密码。
403	用户无该产品权限，提示申请权限。
404	用户产品权限过期，提示续期。
405	机器超过绑定限制，客户端提示解除机器绑定。
501	已经接收客户端的请求，但是客户端的秘钥已经过期，需要使用新的秘钥重新

	进行请求。
503	服务器内部发生异常无法满足请求，需要客户端切换其他服务器进行请求。

2.2.3 第三方认证授权交换信息

系统支持第三方登陆认证授权，第三方登陆认证授权需要提供 HTTP 或者 HTTPS 的方式进行登陆认证授权，在客户端到 AuthServer 端采用本系统中的 RSA 和 AES 加密的方式进行。对于 HTTP 的方式，采用原始信息转发的方式进行(RSA 和 AES 解密后的数据)，对 HTTPS 的方式则采用默认的证书认证传输。任何第三方登陆认证的系统必须返回如下结构

```
{
"Code":"XXXX",
"UserCode":"XXXX",
"ExtInfo": []/{}/""
}
```

Code:状态码，参考 2.2.2 状态码定义

UserCode:在本系统中登记过的用户编码

ExtInfo:第三方系统中的扩展信息，会返回给调用者。