**太平洋保险**

**集团账号权限管理平台建设项目**

**解决方案**

文档历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 日期 | 版本 | 文件状态 | 参与者 | 作者 |
| 2013-12-31 | V1.0 | 完成初始版本 |  | 王沐寰 |

# 文档概述

## 编写目的

本文档对CPIC账号权限管理的现状、需求、设计实现进行了描述。对相应的解决方案进行了分析和规划。

本文档将作为从解决账号权限的相关系统的进一步设计，规划的参考；

## 术语和定义

1. 用户：指使用公司信息系统的人员；
2. 内部员工：以个人身份和公司签订正式劳动合同，由人力资源部集中管理的人员；
3. 外部人员：没有以个人身份和公司签订正式劳动合同的人员
4. 主账号：指用户在系统中的身份管理标识，与实际人员一一对应；
5. 从账号：指用户具体使用某设备或信息系统的主体；
6. 权限：指能够访问的信息系统资源和操作等；
7. 角色：是一个表达访问控制策略的语义结构，它可以表示承担特定工作的资格，一般一个角色是数个系统权限的组合；
8. 岗位职责：指用户在各业务部门中真实的工作内容或角色，各业务部门在人力资源部定义的岗位职责基础上根据实际的工作分配进行细化；
9. 岗位职责矩阵：体现用户及其对应的岗位职责关系的列表；
10. 认证：通过有效的行为或流程操作来确认访问系统主体的身份真实性；
11. 授权：通过有效的行为或流程操作来决定，访问系统主体按照相关岗位职责或制度被许可访问什么样的资源及进行什么样的操作。

# 太保帐户及权限管理现状

## 表现

目前主账号开设主要有几种模式，

第一种是通过REMEDY工单的形式，工单如果由个人发出，则附上审批表，如有应用系统维护人发出则不需要审批表，P13维护人员根据工单手工建立主账号，如果工单中描述了该用户需要的应用权限，则同时把赋予相应应用权限。如果P13系统和对方应用系统有建立了账号管理接口，则会自动把P13账号再推送到对方系统，当P13账号发送变更或销户时也会作同样的动作。如果没有系统自动同步接口的，则通过工单再转回到应用系统，有应用系统根据P13反馈的信息进一步建立P13和应用系统的管理，整个流程操作完成。

第二种模式，业务系统先建立了从账号（应用账号），P13系统自动从业务系统获取新建或注销账号的信息，由于双方系统没有事先约定的唯一标识，P13获取到数据后，只能人工判断处理这些账号。

## 问题、缺陷

可以看出，通过这些处理机制，有几个问题：

1. 所有账号的开始并没有明确的管理流程，没有明确的人员进行管理，P13维护人员只能被动的根据用户或相关人员提供的信息维护账号，无法对该用户信息的准确性进行判断，比如这个用户是否已经申请过了P13账号，如果判断已经申请过了，是否可以拒绝新账号的开设申请。
2. 通过remedy的机制无法严格保证账号处理的过程准确，可控，可审计，容易由于人为因素导致问题。
3. 建立主、从账号,，及两者建立关系的过程多种多样，不可控制，导致目前一个多号，孤立账号等等现象。
4. 对于权限的管理完全有应用系统自己控制，也导致账号的权限无法有效管理，一个用户根据他的岗位到底应该有哪些权限，一个用户转岗、离职时权限是否及时得到相应处理，都没能有效的管理和控制。

由于以上的种种缺陷，导致目前公司账号大量冗余，权限不清，也无人能说清整个公司账号权限的真实情况。

# 账号权限的未来管理及目标

## 账号权限有效管理的目标

* 账号集中有效管理，主要体现在

1. 用户基本信息来源必须准确，主要包含姓名、证件号码、机构、部门、岗位，用户状态。
2. 根据基本信息，产生用户的唯一的主账号
3. 根据主账号，产生业务系统的唯一从账号
4. 主账号及从账号的产生都必须经过有效可控的审批控制。

* 权限集中有效管理，主要体现为

1. 建立岗位职责和应用系统角色，权限的对应关系，即授权标准
2. 权限的变更必须经过有效的审批控制

通过以上两点，最终对用户的账号权限模型如下：



一个用户拥有一个主账号，一个主账号对应多个从账号，每个从账号对应一个应用系统，相应的对应了这个系统内的权限集。（是否存在无法做到一人一号机制的应用系统，如某一用户需要访问山东的业务数据，需要登录类似于严格区分地域的账号SD\*\*\*\*，而要访问四川的业务数据，需要登录SC\*\*\*的账号。这样该用户则需要拥有多个从账号）。

## 有效的审批控制

要想达到我们的管理目标，需通过有效的管理流程来实现，需要对一个用户在太保的生命周期的管理的每一个环节都做到有效控制，从业务上说需要有三个方面，一个是有审批流程的参与者，一个是审批流程的过程，最后是一个用户获得的相应的账号权限后，用户使用的流程控制

### 流程参与者

根据《太保集团信息系统用户管理流程.doc》的规定，参与者有如下几个职责角色：

* 申请用户

申请用户是应用系统账号权限的申请的提出人，也是应用系统的最终使用人。

* 申请用户主管

申请用户的直接主管是权限申请的审批人和责任人；

* 用户管理专员：

用户管理专员是账号权限管理总的管理人员，负责收集、复核、记录、分发本公司所有的账号权限申请，负责维护所有应用清单，内部员工基本应用系统清单，安排账号权限的定期清理计划。

* 应用管理员

应用管理员为应用系统中进行人员账号权限日常管理的操作人员，账号权限的日常管理操作包括账号的创建、删除、人员基本信息的变更录入、权限变更等。

* 人力资源部

人力资源部是提供内部员工基本信息的权威部门，是人员入职、人员离职、人员转岗的信息提供部门，也是账号定期清理的发起部门及审核确认部门，有例外申请的复核否决权，对检查中发现的违规问题，追究相关部门和人员的责任，是最终的责任追究部门。

### 审批流程（从《太保集团信息系统用户管理流程.doc》摘录）

主要有一下三个流程

* 人员入职



|  |  |
| --- | --- |
| 流程描述 | 新加入公司内部员工依照本流程描述开设内部员工基本应用系统账号。 |
| 输入 | 用户基本信息，包括人员姓名，身份证号码，所在部门，工号，岗位。  人力资源部人员入职证明。 |
| 输出 | 人员主账号，创建基本应用系统账号和权限。 |
| 执行策略 | 所有新加入公司人员依据人力资源部人员入职证明，按照此流程开设内部员工基本应用系统账号，内部员工基本应用系统包括：1、P13，2、OA，3、P07，4、Proxy，5、集团EHR，6、内部网站 |

* 从账号新增和权限变更



|  |  |
| --- | --- |
| 流程描述 | 本流程描述员工申请新应用账号或申请变更应用系统权限。 |
| 输入 | 用户基本信息，包括人员姓名，身份证号码。  账号新增和权限变更审批证明。 |
| 输出 | 账号创建，权限变更，或申请否决告知。 |
| 执行策略 | 1、除员工入职时人力资源部授权为新员工开设的账号外，所有应用系统的账号新增或权限变更都需要遵照此流程执行。  2、外部人员申请账号，必须有用人部门员工推荐担保，除填写用户基本信息外，还应注明申请账号有效期限。 |

* 人员离职



|  |  |
| --- | --- |
| 流程描述 | 离职人员依照本流程描述完成应用系统账号权限处理。 |
| 输入 | 离职用户基本信息包括：人员姓名，身份证号码，所在部门。  人力资源部人员离职证明。 |
| 输出 | N/A |
| 执行策略 | 所有离职内部员工都需要执行此流程。 |

* 人员转岗



|  |  |
| --- | --- |
| 流程描述 | 转岗人员依照本流程描述完成应用系统账号权限处理。 |
| 输入 | 转岗用户基本信息包括：人员姓名，身份证号码，原部门，转往部门，原岗位，现岗位，转岗时间。  人力资源部人员转岗证明。 |
| 输出 | N/A |
| 执行策略 | 所有内部员工转岗都需要执行此流程。 |

## 用户对账号权限使用的过程控制

通过合理的流程控制，使得用户账号及权限得到有效管理，用户获得了账号和权限的资源，则用户在在使用这些资源的过程中需要得到相应的认证及权限控制，认证及权限控制流程图如下：



# 解决方案

## 方案解决思路

逻辑图：



说明：

1、用户通过统一身份管理进行账号和权限认证后正常使用应用系统

2、通过内部人员HR系统和外部人员系统(是否存在）提供基本信息的校验和交互

3、账号权限管理系统提供申请、变更、注销等流程审批的操作信息，并提供数据供展示报表或分析

总体架构模型的提供一个简单明了、清楚而易于理解的模型，帮助项目组成员就目标系统的总体架构设计达成共识。

## 方案详述

### 方案的前提、基础、以及约束

由于解决方案是在目前的实际情况上来解决，首先需要公司在这方面有明确可实施的管理规定和业务规则，目前规则已经基本制定完成；其次需要考虑目前和账号权限管理相关的系统情况；最后需要考虑将来可持续性的改进和易于维护的问题。

#### 业务规则建立

用户的账号权限管理根据《用户管理规范》已经对用户、主账号、从账号、权限等进行了准确的定义，并对用户账号及其权限的管理提出了明确的要求；为了实现账号权限管理的要求，在《用户管理流程》中也对账号权限的管理流程做了详细规定。IT解决方案以这个规范要求和流程规定为依据，进行合理设计。

#### 目前P13系统

目前太保依据在2007年实施了P13系统，对用户的账号、权限、统一认证等进行了一定的管理和控制，P13主要是基于IBM 的Tivoli IM/AM产品，其中IM是用户的身份管理，AM是访问策略控制，访问策略主要包括了访问控制列表（即控制可访问的应用系统），访问时间控制，访问密码控制，访问的本地资源控制等待，但是无法管理用户在一个应用系统内部的权限，比如AM可以管理一个用户是否有登录财务系统的权限，或在什么时间内登录财务系统的权限，但无法管理这个用户进入财务系统内部后，具体有那些权限，也无法在AM中对用户来授予某个应用系统内的权限，所以AM对这方面的管理是比较弱的，无法达到太保对权限的控制需求，即可以统一、集中、有效的管理一个用户在任一应用系统中具有的角色，或菜单功能，或可访问的数据范围等具体的权限项，这也正式权限管理的核心内容。

P13目前主要的实现的功能如下：

1. 用户身份统一管理，创建用户的主账号，并和用户一一对应，通过身份证确定用户的唯一性，以及对用户的其他信息和密码进行管理。
2. 应用权限的分配，可以对主账号分配应用系统，即建立和应用系统的对应关系，但不能具体分配应用系统内部的具体权限项。
3. 支持用户的统一认证和单点登录的过程。
4. 支持其他的访问策略，例如访问时间控制、访问控制列表、访问密码控制等。



#### 寿险集中授权系统

由于当前各个系统的授权流程多样，方式复杂，造成用户对权限申请流程不明确，对系统的权限组成不了解，申请权限不便，处理周期延长。并且造成用户在系统中的授权信息散落在各个系统中，无法控制不同系统之间的授权冲突，无法对用户的授权信息进行分析，并进一步做好风险把控。

基于此，需要设计开发一套符合业务功能的应用系统，以实现统一平台、统一流程的集中授权机制，这就是寿险集中授权系统开发的业务背景。

目前寿险集中授权系统已经在投入使用，主要有三方面的成果：

1. 促使业务管理部门整理出所有的作业角色/岗位，并明确这些作业角色/岗位的应用系的权限；
2. 促使业务管理部门定义出各种作业角色/岗位/权限的申请审批流程
3. 审批通过的权限指令集通过有效的方式控制应用系统按这些指令集赋予用户权限
4. 通过以上几方面，使得权限的定义，权限的申请审批得到有效管理、控制，并可以有统计报表 日志等供审计或分析，提高公司的管理水平。

该系统主要流程如下：



可以看到，授权系统发出权限包给应用系统，应用系统按照权限包信息自动设置权限，这是授权系统的最终目标，但在这个过程，由于应用系统的原因暂时不支持，可以权限包可以体现为一个XLS表格，有应用管理人员手工进行权限的设置。

#### 可支持持续改进、维护分析

通过以上的分析，为了达到太保账号权限的管理要求，需要有统一的身份管理（即账号管理），统一的授权管理，统一的身份认证和单点登录控制，以及授权以外的登录策略管理。IM/AM除了统一的授权管理难以实现外，其他几项都是IM/AM的标准功能，在目前的P13上已经实现。统一授权管理和被授权的应用系统耦合关系较为密切，和公司对授权的管理流程，权限（具体体现未作业角色或岗位）等的定义，具体如何授权等等不同业务要求的相关性也很大，不同的要求将得到不一致的统一授权系统，所以通过IM/AM这种固化的产品来充分满足太保的需求，会有比较大的障碍。

通过自主开发的统一授权系统，可以充分满足业务的各种需求，在权限管理逐渐深化的过程中，会不断的优化授权过程，优化应用权限的定义，优化用户职责岗位的定义，不不断的有更细腻的需求，可以想象，这将是公司管理逐步规范，公司管理能力，管理水平逐步提高的过程。

统一授权系统可以在目前寿险的经验和基础上进一步优化，改造，提出更合适的满足全司范围授权需要的系统。

### 解决方案的关键要素分析

根据《太保信息系统用户管理规范》有如下关键要素，本文也在“1.3术语和定义”中进行了描述：主账号、岗位职责、角色、从账号、权限。它们之间的关系用如下示意图表示：



每个用户全司有唯一的主账号，每个用户通过岗位职责的定义得到角色，每个角色有多个从账号，每个从账号在每个应用系统中有若干个权限集。这样就构成了一个用户在公司内准确拥有了账号资源和权限资源。

### 用户统一认证和单点登录分析

当用户拥有了账号资源和权限资源后，如何可以方便、有效、合理的使用这些资源？这就是通过统一身份认证和单点登录功能来协助用户的使用其拥有的资源。



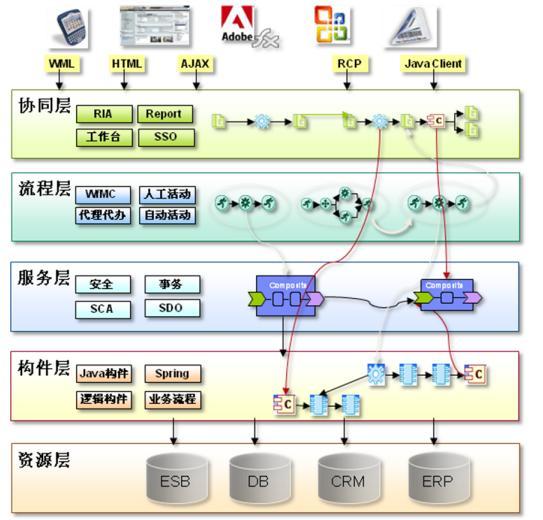
## 架构设计详述

### 基本原则

1. 以业务需求为指导，以满足当前和未来的业务需求，具备前瞻性、先进性。
2. 满足功能性需求和非功能需求。
3. 架构设计采用层次性的体系架构，减少与其它业务模块间的耦合性，使系统具有灵活性，扩展性。
4. 系统规范对其他业务系统服务接口的设计，以实现通用性、灵活性。
5. 系统的建设应符合CPIC的IT策略、应用架构、信息模型和其他统一标准。
6. 实用性原则，避免“过度设计”。
7. 满足复用的要求，最大程度的提高开发人员的工作效率。

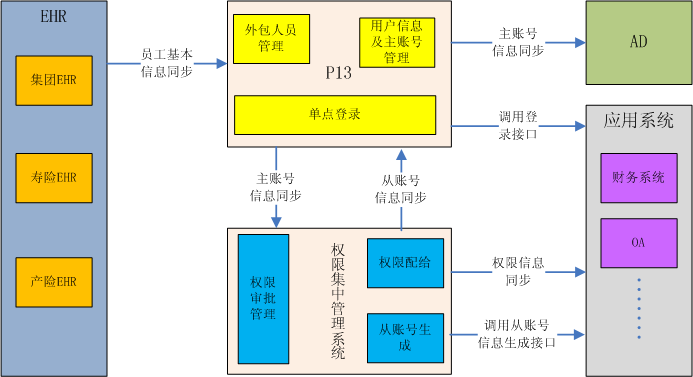
### 软件平台及框架

系统将采用EOS平台，并基于EOS Platform版本中的工作流设计、开发、管理业务流程，UI将主要采用JSP技术。



## 总体结构与模块

### 系统架构图及说明





相关说明：

1、用户通过桌面AD访问P13系统

2、P13通过IM和AM验证后，显示用户能看到的AppList图标应用

3、点击应用访问具体应用系统

P13与账户权限管理系统（包括流程，HR系统之间的交互）的架构图



1、P13与EHR通过接口进行数据同步

2、P13通过单点登录访问账号权限管理系统

3、账号权限管理系统的业务功能模块调用工作流引擎进行申请审批

4、审批后的生成的权限数据通过自动化接口发送给P11或EAI系统

5、P11/EAI与需自动化接入的应用进行交互并将结果返回给账号权限管理系统



统一认证系统改为IM 和SSO

各系统定位：

* HR系统：负责公司员工的基本信息的准确性，这些信息主要为：用户姓名、证件号码、机构、部门、岗位、用户状态。
* 统一认证系统：负责维护用户的主账号，并把主账号信息传输给AD和统一授权系统；负责除应用权限外的策略控制，负责用户的统一身份认证和单点登录。
* 统一授权系统：负责用户的应用权限变更的申请和审批；维护从账号及其对应的应用系统权限；建立主账号和从账号的对应关系，同时把这种关系传输到统一认证系统。
* AD：根据用户所属的机构、部门、岗位等，负责控制主账号对应的WIN桌面的权限
* 普通应用系统：负责接受统一授权系统的指令，实现从账号及其对应的权限。

### 系统架构设计描述

#### 开发视图



#### 逻辑视图



#### 进程设计



#### 物理视图



### 统一授权系统和应用系统的关系

#### 如何授权

当用户的权限审批在统一授权系统中通过后，如何在对应的系统中实现，支持如下两种方法

（1）、通过人工的方法，根据这些权

审批信息，在对应的系统中手工授权，保证和审批的权限一致。

（2）、通过系统的方法，由统一授权系统直接发交易给应用系统，应用系统自动实现权限的分配。

由于第二步是个比较复杂的过程，对被授权的应用系统的要求很高。

#### 从账号如何产生

1. 一般情况，从账号由【统一授权系统】按设置好的规则集中生成。
2. 如果必须由应用系统自己产生从账号，则应用系统提供产生从账号的接口，由【统一授权系统】调用生成从账号。

## 账号权限流程图

在IT系统架构确定的情况下，根据《太保集团信息系统用户管理流程.doc》，共有7个流程：人员入职、账号新增和权限变更、人员离职、人员转岗、定期清理、例外申请、检查处罚等流程从系统的角度做个描述。

### 人员入职流程



基本应用主要指【OA】,【P07的网上保险】、【人力资源】等，是在创建主账号时，系统自动申请这些系统应用的权限。

账号权限管理系统是基于岗位来授权的，是否需要将基本应用系统的申请纳入到统一授权系统中来统一管理？

### 从账号新增和权限变更



（1）、用户直接向【统一授权系统】提出权限申请，前提是：该用户对应的主账号已经在【统一授权系统】中存在。

（2）、【统一授权系统】审批通过后，通知应用系统修改权限

（3）、如果该从账号已存在，调整从账号的权限则不必通知到P13，如果是新增从账号或注销从账号，则通知到P13，主要接口信息有：主账号、从账号、状态（新增、注销）。

### 人员离职



（1）、用户提出离职申请，HR把该用户职位“待离职”状态

（2）、HR把该用户待离职信息发送给统一认证系统

（3）、同时管理专员也收到用户的离职申请，此时统一认证系统开始发起注销主、从账号的业务

（4）、统一认证系统发起注销所有从账号的请求，发送给统一授权系统，

（5）、统一授权系统向每个应用系统发送注销从账号的请求

### 人员转岗



（1）、对于人员转岗，对从账号存在两种处理情况，一种是需要将应用系统的从账号全部删除再重新建立新的从账号及权限信息，一种是保持从账号信息不变，只是更改从账号所对应的权限。这个需要根据不同的应用系统要求而定。

（2）、如果该从账号已存在，调整从账号的权限则不必通知到P13，如果是新增从账号或注销从账号，则通知到P13，主要接口信息有：主账号、从账号、状态（新增、注销）。

### 定期清理

（1）、授权系统管理员发起定期清理流程，从HR系统中同步用户信息并对机构、部门、岗位等信息进行比对，

（2）、对两系统不一致的信息记录并生成相应文件

（3）、线下确认不一致的信息，如果确认以HR系统的为准，而授权系统没有更新的，需要及时通知统一认证和应用系统进行更新。

### 例外申请



（1）、对于用户需要使用不符合岗位权限定义的应用权限，需要额外提出审批。

（2）、人力资源有例外申请的复核否决权。

（3）、通知应用方更新权限信息。

（4）、如果该从账号已存在，调整从账号的权限则不必通知到P13，如果是新增从账号或注销从账号，则通知到P13。

## 外部用户管理

由【统一授权】进行管理，外部用户信息通过【统一授权】进行一定的流程管理后保存在P13系统，并生成主账号，后续的从账号以及对应的权限管理和内部员工的系统处理过程一致。

# 目前项目进展

## 系统接入情况

目前，帐号权限管理系统已经上线试运行

产险、寿险、集团、资产公司所属系统的接入数目情况如图所示：

其中大部分系统都是通过发送流程申请单申请发送工单实现了审批后自动化处理开权限的功能

## 系统截图展示































